

FUTURE ARCHITECTURE FOR NAS COMMUNICATIONS

CNS-ATM TASK 11

PREPARED FOR:

**FEDERAL AVIATION ADMINISTRATION
ASD-120/140
800 INDEPENDENCE AVENUE, S.W.
WASHINGTON, DC 20591**

PREPARED BY:

**ITT INDUSTRIES
ADVANCED ENGINEERING AND SCIENCES DIVISION
1761 BUSINESS CENTER DRIVE
RESTON, VIRGINIA 20190-5337**

ACKNOWLEDGEMENTS

This study effort was conducted for the Federal Aviation Administration's Office of System Architecture and Investment Analysis (ASD). Mr. Leon Sayadian of ASD-140 formulated the technical requirements of this task and provided leadership in its conduct. Ms. Ann Tedford (ADS-140), Mr. John Horrocks, (ADS-120) and Ms. Laura Hamman (ASD-120) provided technical oversight and guidance throughout the course of the study.

TABLE OF CONTENTS

SECTION	PAGE
1.	INTRODUCTION..... 1-1
1.1	Background1-1
1.1.1	Challenge Faced by the FAA1-1
1.1.2	FAA’s “Program” Approach to Providing Communications.....1-1
1.1.3	FAA’s FTI Initiative1-1
1.1.4	Summary of Work to Date1-2
1.2	Objectives and scope of the Study1-3
1.3	Organization of this report1-3
1.4	List of Documents1-5
2.	KEY TECHNOLOGY, PROTOCOLS, AND STANDARDS FOR SUPPORTING SERVICES..... 2-1
2.1	Technology, Protocols, and Standards for QoS Provisioning2-1
2.1.1	Ipv6 Supports QoS Provision for Bandwidth Reservation.....2-3
2.1.1.1	Static Reservation.....2-3
2.1.1.2	Dynamic Reservation2-3
2.1.2	Provision for High Availability.....2-3
2.1.2.1	Physical Layer Redundancy2-4
2.1.2.2	Network Layer Redundancy2-5
2.1.2.3	Network Robustness During Failures2-5
2.1.3	Provision for Low Data Delay and Delay Jitter2-6
2.1.4	Provision for High Probability of Packet Delivery2-6
2.2	Technology, Protocols, and Standards for Information security2-6
2.2.1	Need For Security2-6
2.2.2	Security Solutions2-7
2.2.3	IPSec2-9
2.2.3.1	IPSec Architecture2-9
2.2.3.2	IPSec Authentication.....2-10
2.2.3.3	IPSec ESP2-11
2.2.3.4	IPSec Key Management.....2-12
2.2.4	Virtual Private Networks.....2-13
2.2.5	VPN Access Control - Firewalls2-15
2.2.5.1	Types of Firewalls.....2-15
2.2.5.2	Firewall Architectures.....2-17
2.3	Technology, Protocols, and Standards for Voice & Video over Fast Packet Networks2-19
2.3.1	Voice and Video Services2-19
2.3.2	Applicable Standards and Protocols.....2-19

TABLE OF CONTENTS (Cont'd)

SECTION	PAGE
2.3.2.1	H.323.....2-21
2.3.2.2	SIP2-24
2.3.2.3	MGCP2-25
2.3.2.4	Comparative Analysis of VoIP Protocols2-26
2.3.3	Technology and Market Trends2-28
2.4	Technology, Protocols and Standards for Enterprise Management2-28
2.4.1	Introduction2-28
2.4.2	Network Monitoring and Management2-29
2.4.3	Management of IP Address Space2-30
2.4.3.1	Allocation of IP Addresses to Facilities/Programs and Hosts.....2-31
2.4.3.2	Management of the System of Registering Names for Internet Users2-31
2.4.3.3	Operation of the Root DNS Server System.....2-32
2.4.3.4	IPv6/IPv4 Address Resolution2-32
2.4.4	Time Distribution Services2-35
2.4.4.1	Synchronization Basics2-35
2.4.4.2	Network Synchronization – NTP2-36
2.4.5	Network Directory Services.....2-39
2.4.5.1	Definitions.....2-39
2.4.5.2	Characterizations.....2-40
2.4.5.3	Need for Common Directories2-41
2.4.5.4	Network Directory Service Standards.....2-41
3.	COMPARATIVE ANALYSIS OF FAA COMMUNICATIONS SERVICE NEEDS VS. AVAILABLE SERVICES AND TECHNOLOGIES 3-1
3.1	Data Delivery Services.....3-1
3.1.1	FAA Needs.....3-1
3.1.1.1	Bandwidth3-1
3.1.1.2	Availability.....3-2
3.1.1.3	Latency3-2
3.1.1.4	Packet Loss.....3-2
3.1.2	Delivered Performance of Commercial Data Delivery Services.....3-3
3.1.2.1	Overview of Communications via Packet Networks3-3
3.1.2.2	Bandwidth Over a Packet Network.....3-6
3.1.2.3	Availability Over a Packet Network3-6
3.1.2.4	Data Delay Over a Packet Network3-6
3.1.3	Comparison of FAA Needs with Available Packet Services3-7
3.1.3.1	Bandwidth3-7
3.1.3.2	Availability.....3-7

TABLE OF CONTENTS (Cont'd)

SECTION	PAGE
3.1.3.3	Data Delay.....3-8
3.2	Voice/Video3-8
3.2.1	FAA Service Needs.....3-8
3.2.1.1	Voice3-8
3.2.2	Delivered Performance of Available Services3-10
3.2.2.1	Dropped Packets.....3-10
3.2.2.2	Latency3-11
3.2.2.3	Echo3-16
3.2.2.4	Jitter Buffering3-18
3.2.2.5	Vocoder Selection3-18
3.2.3	Comparison3-19
3.3	Security3-20
3.3.1	FAA Information Security Requirements3-20
3.3.1.1	Applicable Information Systems Security Program Requirements.....3-20
3.3.1.2	Applicable Information System Security Architecture Requirements3-21
3.3.1.3	Applicable Wide Area Network Security Requirements3-29
3.3.2	Applying Security Technologies to FAA Security Requirements3-29
3.4	Enterprise Management3-30
3.4.1	Introduction3-30
3.4.2	Network Monitoring and Management3-30
3.4.3	Management of NAS IP Address Space3-31
3.4.3.1	FAA Allocation of IP Addresses to Facilities/Programs and Hosts.....3-32
3.4.3.2	Adoption of a Naming Convention that Maps Names to IP Addresses3-35
3.4.3.3	Implementation of the Domain Name System (DNS): Location and Number of Domain Name Servers3-36
3.4.4	Network Time Distribution3-37
3.4.4.1	Time Distribution Service Requirements in the NAS.....3-37
3.4.4.2	Application of Time Distribution Technologies to the NAS3-37
3.4.5	Network Directory Services - NAS Common Directory Service.....3-38
4.	APPLICATION OF AVAILABLE SERVICES/TECHNOLOGIES TO ZOB 4-1
4.1	Overall Architecture Description4-1
4.2	Description of Commercial Managed Backbone Networks.....4-2
4.2.1	General Architecture and Performance4-2
4.2.2	Trends.....4-3
4.2.3	Defining Backbone Network Scenarios for Study4-3
4.2.3.1	Low Density POP Backbone.....4-4

TABLE OF CONTENTS (Cont'd)

SECTION	PAGE
4.2.3.2	High Density POP Backbone4-5
4.3	ZOB Facilities Selected for Analysis4-5
4.3.1	Selection Process.....4-5
4.3.2	FAA Programs Represented by the Selected Facilities.....4-6
4.4	ZOB Nodes Definition and Communication Requirements.....4-8
4.4.1	Grouping ZOB Facilities into Nodes4-8
4.4.2	Local Node Communications.....4-10
4.4.2.1	Campus Network Development Methodology.....4-12
4.4.2.2	Campus Area Network Concepts4-13
4.4.3	Bandwidth and QoS Constraints by Node.....4-16
4.4.3.1	Bandwidth Determination by Node.....4-17
4.4.3.2	Latency Determination by Node4-19
4.4.3.3	Availability Determination by Node4-19
4.4.3.4	Diversity Determination by Node4-20
4.5	Connecting Nodes to Backbone Networks.....4-20
4.5.1	General Architecture Concepts4-20
4.5.1.1	Scenario 1A: All Nodes Connect Directly to the Low-Density POP Backbone.....4-20
4.5.1.2	Scenario 1B: Regional FAA Hubs Connect to a Low-Density POP Backbone.....4-21
4.5.1.3	Architecture Scenario 2: Connecting All Nodes Directly to the High-Density POP Backbone4-22
4.5.2	Connection Technology4-23
4.5.2.1	Existing Technology and Trends4-23
4.6	Network Equipment at FAA Nodes and Network Circuits4-25
4.6.1	Customer Premise Equipment.....4-25
4.6.2	Network Circuits4-29
5.	EVALUATION OF THE ZOB ARCHITECTURE..... 5-1
5.1	Transition Issues associated with ZOB Architecture5-1
5.1.1	Current NAS Voice Equipment and Interfaces5-1
5.1.2	VSCS.....5-3
5.1.2.1	VSCS Signaling Interfaces.....5-3
5.1.2.2	Functionality Provided by the VSCS5-7
5.2	Integration/Transition to VoIP5-9
5.2.1	Transition States.....5-12
5.2.2	End State5-13
5.2.3	Transition Issues/Problems5-16

TABLE OF CONTENTS (Cont'd)

SECTION	PAGE
5.3	Performance Assessment5-17
5.3.1	Latency5-17
5.3.2	Availability Calculation5-21
5.3.2.1	Box Reliability5-21
5.3.2.2	Network Availability.....5-22
5.4	Cost Analysis and Comparison5-28
5.4.1	Focus of the Cost Analysis.....5-28
5.4.2	Circuit Cost Calculations5-28
5.4.2.1	Baseline Communication Architecture Circuit MRC5-29
5.4.2.2	Network Architecture Scenario 1A Circuit MRC5-31
5.4.2.3	Network Architecture Scenario 1B Circuit MRC5-33
5.4.2.4	Network Architecture Scenario 2 Circuit MRC.....5-33
5.4.3	Backbone Usage Costs and Other Cost Considerations5-35
5.4.3.1	Backbone Network Usage Charges.....5-35
5.4.3.2	Network Access Charges for Distance Circuit End-Points5-38
5.4.4	Total Circuit MRC for Architecture Scenarios5-39
5.4.5	Circuit NRC and CPE Cost Considerations5-39
5.4.5.1	Circuit Non Recurring Costs5-39
5.4.5.2	Customer Premise Equipment Costs5-40
5.4.6	Cost Summary5-43
6.	CONCLUSIONS AND RECOMMENDATIONS 6-1
6.1	Work Summary6-1
6.2	Conclusions6-1
6.3	Recommendations6-4
	LIST OF ABBREVIATIONS, ACRONYMS AND CODES.....AA-1
	ENDNOTES..... EN-1
	APPENDIX A: FAA TELECOMMUNICATION SERVICE
	CRITICALITIES AND DIVERSITY PRIORITIES.....A-1
	APPENDIX B: NODE DIAGRAMS FOR BASELINE, SCENARIO 1A,
	SCENARIO 1B, AND SCENARIO 2 ARCHITECTURES.....B-1
	APPENDIX C: ARCHITECTURE CIRCUIT LISTS.....C-1
	APPENDIX D: LATENCY AND AVAILABILITY CALCULATIONS...D-1

LIST OF FIGURES

FIGURE		PAGE
2.1-1	Example Communications Protocol Stack.....	2-4
2.1-2	SONET 4 Fiber Bi-directional Line Switched Ring (4F-BLSR)	2-4
2.1-3	Robustness of Backbone Communications Between Points B and C.....	2-5
2.2-1	Security Solutions in the TCP/IP Layers	2-8
2.2-2	IPSec Security Architecture (RFC 1825).....	2-10
2.2-3	VPN Topology.....	2-13
2.2-4	Encapsulation in the IPSec Tunneling Mode ESP	2-14
2.2-5	Dual-Homed Gateway Firewall	2-18
2.2-6	Screened Host Firewall.....	2-18
2.2-7	Screened Subnet Firewall	2-19
2.3-1	System Control, Audio, Video, and Data Specifications of H.323.....	2-21
2.3-2	H.323 Architecture	2-22
2.3-3	H.323 Architecture Relationship to the H.32x Standards Universe	2-23
2.3-4	SIP Architecture.....	2-25
2.4-1	Network Monitoring and Management Configuration	2-30
2.4-1	Tunneling Scenarios	2-33
2.4-2	Encapsulation Process.....	2-34
2.4-3	NTP Architecture.....	2-37
2.4-4	NTP Protocol Header and Timestamp Formats	2-38
2.4-5	NTP Configuration	2-39
2.4-6	Directory Client/Server Interaction	2-40
3.1-1	Illustration of POPs and Access Lines for Network Service	3-5
3.1-2	Example Structure of Network Cloud (AT&T IP Network)	3-5
3.1-3	Data Delay Over a Network.....	3-7
3.2-1	Subjective Evaluation of Speech Quality as a Function of Pure Delay	3-9
3.2-2	Voice Quality as a Function of Packet Loss Rate.....	3-11
3.2-3	The Impact of Link Capacity on Queuing Delay.....	3-13
3.2-4	The Impact of Constant Bit Rate (CBR) Link Sharing on Queuing	3-13
3.2-5	Encapsulation of Vocoder Packet, Showing Overhead With and Without Header Compression.....	3-15
3.2-6	Impact of Header Overhead on the 99.9 Percentile Delay Bound	3-15
3.2-7	Measured End-to-End Latency Values for Various VoIP Implementations.....	3-16
3.2-8	Required Echo Suppression as a Function of Absolute Delay.....	3-17
3.3-1	Common Network Security Interface	3-23
3.3-2	Firewall Based VPN	3-25
3.3-3	Common Network Security Model.....	3-27

LIST OF FIGURES (Cont'd)

FIGURE	PAGE
3.4-1	Telecommunications Architecture, Showing Enterprise Management Elements3-31
3.4-2	FTI Concept of Collection of Network Management Information3-32
3.4-3	FAA Name Space Domain Structure3-35
3.4-4	Location and Number of DNS Servers3-36
4.1-1	Overall NAS Architecture Vision4-1
4.3-1	Subset of ZOB Facilities Selected for Analysis4-6
4.4-1	Facilities in the DTW Airport Region4-10
4.4-2	TRACON/ATCT Campus Area Network Components4-14
4.4-3	ARTCC Campus Network4-16
4.5-1	Architecture Scenario 1A Node Connections4-21
4.5-2	Architecture Scenario 1B Node Connections4-22
4.6-1	Mansfield TRACON Baseline4-27
4.6-2	Mansfield TRACON Scenario 1A4-27
4.6-3	Mansfield TRACON Scenario 1B4-28
4.6-4	Mansfield TRACON Scenario 24-28
5.1-1	Overview of the NAS Showing Legacy Voice Switches5-2
5.1-2	VSCS System Architecture5-4
5.1-3	Simplified VSCS Interface Diagram5-5
5.1-4	VSCS Trunk Interface Summary5-6
5.2-1	ZOB ARTCC to ARTCC Interphone Connectivity (SVFA)5-10
5.2-2	ZOB ARTCC to Non-ARTCC Interphone Connectivity (SVFB)5-10
5.2-3	RCAG and BUEC Connectivity to ZOB5-11
5.2-4	Notional ARTCC Transition Architecture5-12
5.2-5	VSCS Console Equipment Interface Diagram5-15
5.2-6	Notional ARTCC End State Architecture5-16
5.3-1	Latency Block Diagram - MFD TRACON to MNN RTR5-19
5.3-2	Example Markov State Diagram5-23
5.3-3	Availability Block Diagrams - MNN RTR to MFD TRACON5-25
5.4-1	Allocation of Baseline Circuits (Number of Circuits)5-30
5.4-2	Allocation of Baseline Circuit Costs5-30
5.4-3	Distribution of Operational Circuit Costs5-31
5.4-4	Allocation of Network Access Communication Costs5-36
5.4-5	Cost Summary Data5-43
6.2-1	Alternative Architectures Considered6-3
6.2-2	Monthly Cost of Leased Lines for Baseline and Alternatives6-4

LIST OF TABLES

TABLE		PAGE
2.1-1	Tools for Guaranteeing Key QoS Parameters.....	2-2
2.2-1	Relative Advantages and Disadvantages of Transport Mode Versus Tunnel Mode.....	2-12
2.3-1	Suitability of ATM, Frame Relay, and IP Protocols to WAN, LAN, and Application Telephony Requirements	2-20
2.3-2	H32x Standards Universe	2-23
2.3-3	SIP Bake-offs.....	2-24
2.4-1	Defined IP Private Address Space.....	2-31
2.4-2	Values to Use in IPv4 Header When Encapsulating IPv6 Packet.....	2-34
2.4-3	Stratum Levels	2-36
3.1-1	FAA's Goals for Service Availability	3-2
3.1-2	FAA Goals for Data Latency Due to Communications	3-2
3.1-3	QoS Parameters of Frame Relay Service Offered by Major Providers	3-4
3.2-1	ITU-T Recommendations for Maximum One-Way Delays	3-10
3.2-2	Codec Standards and Associated Delays	3-12
3.2-3	Packet Serialization Delay for Compressed and Uncompressed Headers of Two Recommended Vcoders.....	3-12
3.2-4	VoIP Delay Budget.....	3-16
3.2-5	Coding Standards and Corresponding MOS.....	3-19
3.2-6	Mean Opinion Score Five-Point Scale.....	3-19
3.3-1	CNSM Operation Summary.....	3-27
3.4-1	Private IP Assignments Summary	3-33
3.4-2	Summary of Operational IPv4 Address Allocation	3-34
4.2-1	POPs for Low Density Backbone	4-4
4.2-2	POPs for High-Density Scenario	4-5
4.3-1	FAA Programs Represented by Selected Facilities	4-7
4.3-2	RMA Categories in the FAA Telecommunication Infrastructure (FTI)	4-8
4.4-1	FAA Network Nodes for the Representative Architecture	4-11
4.4-2	TRACON/Tower Communication Groups.....	4-13
4.4-3	Peak Instantaneous Node Bandwidth Requirements	4-18
4.4-4	Latency Constraints Based on Service.....	4-19
4.4-5	Availability and Restoral Time Requirements for NAS Services.....	4-19
4.5-1	Summary of Considered Access Technologies.....	4-24
5.1-1	Major Voice Switching Equipment Currently in Use in the NAS.....	5-2
5.1-2	Existing FAA Trunk Types for ARTCC.....	5-8
5.2-1	VSCS Position-Level Availability Requirements.....	5-11
5.3-1	Latency Analysis Scenarios	5-18

LIST OF TABLES (Cont'd)

TABLE	PAGE
5.3-2	Latency Budget for MFD TRACON to MNN RTR5-20
5.3-3	Latency Calculation Results Summary5-20
5.3-4	Availability Analysis Scenarios.....5-24
5.3-5	Baseline Architecture Availability Calculation5-25
5.3-6	Architecture Scenarios 1A & 2 Availability Calculation5-26
5.3-7	Architecture Scenario 1B Availability Calculation5-26
5.3-8	Availability Analysis Results.....5-27
5.3-9	Availability Calculations - Added Component Redundancy5-28
5.4-1	Excerpt from Baseline Communication Architecture Circuit List with MRC.....5-29
5.4-2	Scenario 1A Pricing Methods and Tools5-32
5.4-3	Scenario 1A Circuits and Prices5-32
5.4-4	Scenario 1B Pricing Methods and Tools5-33
5.4-5	Scenario 1B Circuits and Prices.....5-34
5.4-6	MRC for Node Connection to Backbone POPs (Scenario 2)5-34
5.4-7	Scenario 2 Pricing Methods and Tools5-35
5.4-8	Scenario 2 Circuits and Prices5-36
5.4-9	Backbone Usage Charge Calculation.....5-37
5.4-10	Backbone Usage Cost Development.....5-37
5.4-11	MRC for Distant End-Point Network Access.....5-38
5.4-12	Total Circuit MRC for Baseline and Proposed Architectures.....5-39
5.4-13	Circuit NRC for Proposed Architecture Scenarios5-39
5.4-14	Representative Network CPE and Associated Costs5-41
5.4-15	Proposed Architectures CPE Tally and Costs.....5-42
5.4-16	Cost Summary5-43

EXECUTIVE SUMMARY

This report investigates the challenge faced by the Federal Aviation Administration (FAA) in transitioning from the current telecommunications infrastructure of the National Airspace System (NAS) to a more modern telecommunications service. The primary purpose of this study was to investigate the extent to which the communications requirements of the NAS could be efficiently met by a modern packet communications network.

The current telecommunications structure of point-to-point leased lines and multiple special-purpose FAA owned and operated networks is used as a baseline for determining communications connectivities that must be supported in any new architecture. Previous work that analyzed the required communications capacity is leveraged and expanded to provide a coherent view of the communications requirements of a subsection of the NAS. (In line with previous studies, the ZOB ARTCC airspace was selected for study.)

The assessment of satisfying NAS communications requirements within the framework of a modern packet network was performed at both a general level and a detailed level:

- At a general level, the applicable technologies for modern communications networks were summarized, and the application of these technologies to the NAS requirements was analyzed.
- At a detailed level, alternative communications network designs that support a major subset of the NAS facilities in the Cleveland ARTCC were developed and evaluated with respect to performance versus requirements and cost.

Assessments at both the general and detailed levels indicate that the NAS communications requirements can be met. The major areas of investigation included the ability to provide adequate bandwidth, meet availability and latency requirements, and provide security and enterprise management services.

It was determined that existing and planned commercial communications networks have adequate bandwidth to carry the NAS data traffic. NAS needs for high availability can be met with current and planned service offerings. Current service providers achieve availabilities of 99.999% to 100% over their modern networks with technologies that incorporate “built-in” redundancy and self-healing. For small and remote NAS facilities that require long distance access lines to networks, a 0.99999 availability requirement can only be met by incorporating redundancy in the access lines.

Although the data latency for a packet network will typically be higher than for point-to-point communications, packet communications networks achieve well under the 300 msec maximum allowed for communications latency for critical radar data. For voice carried over a packet network, if the latency allocation to the communications network is much below 150 msec, advancements over the current practice will be required.

A wealth of alternative standards, technologies, and products that will provide adequate security are available for the NAS. However, implementation of a security architecture can lead to increased data latency, increased cost, and a large increase in processing burden at NAS facilities, so it is important that these constraints are recognized in the implementation of NAS security.

Finally, significant enhancements to the current enterprise management strategies of the FAA can be made with a transition to a modern telecommunications structure.

For the detailed assessment, alternative communications network architectures for the Cleveland ARTCC were developed around three alternative scenarios. These three scenarios were as follows:

- **Scenario 1A**

- Assumed a low density of backbone network access locations or Points of Presence (POPs), comparable to the density of POPs that exists today.
- Connected all NAS facilities to the nearest network POP; in the case of small and remote NAS facilities, some of the access lines spanned large distances.

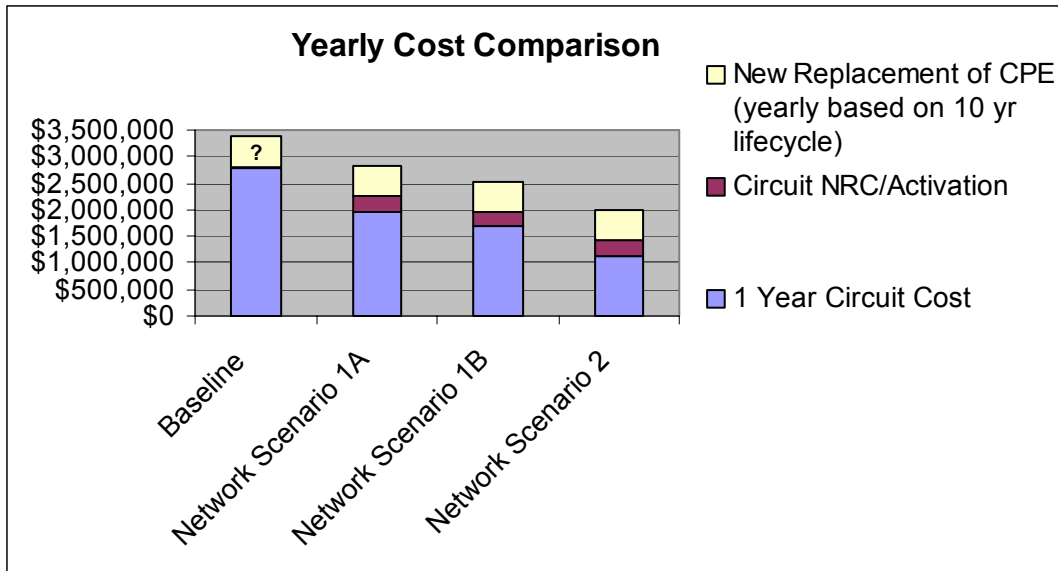
- **Scenario 1B**

- Assumed a low density of network POPs, comparable to the density of POPs that exists today.
- Connected large NAS facilities to the nearest network POP.
- Connected small and remote NAS facilities to the nearest large NAS facility.

- **Scenario 2**

- Assumed a high density of network POPs, comparable to the density of POPs that is projected to exist in the future; this projection was based upon the current density of Internet Service Provider (ISP) POPs (which is quite dense).
- Connected all NAS facilities to the nearest network POP; with the dense POP assumption, even small and remote NAS facilities tend to be close to a network POP.

A detailed cost estimate of the alternative architectures was developed and compared to the baseline of current NAS communications. The figure below summarizes estimates for yearly costs. Note that cost savings are estimated for all the alternatives considered.



Note: Cost for replacement of circuits and equipment for the baseline architecture was not addressed in this study.

It is recommended that the FAA pursue a NAS communications architecture in accord with Scenario 1B above. The rationale is as follows:

- Highly reliable network communications between facilities near network POPs is a mature service that meets FAA needs. Such a network can provide 99.999% to 100% availability of communications between major NAS facilities.
- Maintaining point-to-point links between small/remote facilities and major NAS facilities, for packet communications, is a positive incremental step that affords virtually all the information sharing possible in a packet network, while presenting fewer implementation risks and less of a security challenge than Scenario 1A and Scenario 2.

The FAA should take a uniform and comprehensive approach in application of enterprise management technology and tools to the NAS. In addition to monitoring and control of communications and application network elements, enterprise management should incorporate IP address management; implementation of a domain naming system and servers; directory structures and data warehousing.

In this study, a number of FAA facilities were identified in which different programs in the same location had completely separate communications. Although the economics of doing so were not analyzed, it is believed that there may be great advantage (lower leased communications costs) in implementing “campus area networks” that aggregate data from multiple programs and can share a common access communications to the network.

In summation, it is recommended that FAA migrate toward treating communications and the supporting functions of security and enterprise management as common utilities that provide constant and uniform support across all FAA services.

1. INTRODUCTION

1.1 BACKGROUND

1.1.1 Challenge Faced by the FAA

Telecommunication systems and services supporting every element of the National Airspace System (NAS) are critical to the Federal Aviation Administration's (FAA's) mission. These telecommunications systems are necessary to provide Air Traffic Services (ATS), and to manage, monitor, maintain, and control the NAS. The FAA operates a large and complex telecommunications network. The cost to operate and support this growing network was \$320 million in FY 1997. The cost of operation and supporting the system is expected to grow at a rate of at least 12.5% per year between 1998 and 2003. This growth rate may result in a communications infrastructure that is economically unsupportable¹.

1.1.2 FAA's "Program" Approach to Providing Communications

Historically, each FAA project or program office has developed a required telecommunications infrastructure to support its program. This fragmented development approach has led to an FAA telecommunications infrastructure that consists of a preponderance of point-to-point communication links. Since most of these links are underutilized, this is a very costly and inefficient means of providing enterprise level communications. Furthermore, the FAA has developed a large number of independent networks over the years. Management of multiple networks is necessarily more complex and expensive than managing one integrated network.

1.1.3 FAA's FTI Initiative

In response to Mission Need Statement (MNS) #322, the FAA's Investment Analysis and Operations Research Directorate (ASD-400) formed a team to conduct an analysis of the critical issues set forth in the MNS. The objective of the Investment Analysis Team (IAT) was to recommend a preferred business case solution to support the development of an Acquisition Program Baseline (APB). The IAT considered alternatives to the current approach in which the FAA operates a number of separate networks that support different FAA programs. The IAT study recommended a single network to support all FAA telecommunications: the Integrated Interfacility Services Network (IISN). The IISN would provide for telecommunications transport, switching and routing, as well as network management, control and engineering. The rationale for the IISN was broad based and included superior network management and control, better alignment with the vision of the NAS Architecture (Version 4.0), and lower costs.

The FAA Telecommunications Infrastructure (FTI) program is intended to address future FAA communications requirements in an integrated, comprehensive, and cost-effective manner. To quote the FTI Technical Guidance Document:

“With the FTI, the FAA hopes to achieve an integrated solution that will allow the users to see a single system as their transport provider from desktop to desktop. The FTI will consolidate the NAS operational networks and the mission support networks into a shared network with each being partitioned for security. The FTI will include interfacility, intrafacility, and mobile services².”

1.1.4 Summary of Work to Date

During the past several years, ITT Industries (previously Stanford Telecom) has supported the FAA Systems Engineering Division in developing a vision for the NAS Communications Architecture. Studies have focused on developing communications requirements and the applicability of current technologies for meeting the wealth of communications needs of the NAS. These studies included CNS-ATM Tasks 4, 5 and 10.

The Task 4 study explored the feasibility of the NAS architecture view of a common backbone (possibly Asynchronous Transfer Mode (ATM)) with a consolidation of NAS operational and administrative data and voice traffic. This study compared both backbone and access alternatives. The backbone technologies evaluated were ATM and frame relay. The access technologies evaluated were an extension of the Data Multiplexing Network and frame relay. The study provided cost comparisons and evaluations of the technologies ability to meet the varying performance requirements of the different categories of NAS traffic.

Task 5 developed a detailed understanding of the communications requirements of Air Traffic Control (ATC) automation systems and their attached sensors to provide a basis for development and evaluation of potential communications solutions. The purpose of the task was to provide a time-phased communications requirements set associated with ATC automation systems. The intent was to support an evolution of the current NAS connectivity structure from the current provisioning of numerous point-to-point circuits, to a networked approach that facilitates the delivery of a given set of data to multiple locations.

The Task 10 study extended the work of both Tasks 4 and 5 by further expanding and refining the study of communications requirements through a mixture of simulations, measurements, and analysis; and then developing a replacement architecture with a hierarchical backbone structure and access methods. A complete reference requirements set was developed for major NAS facilities, including Air Route Traffic Control Centers (ARTCCs), Terminal Radar Approach Control Facilities (TRACONs), Airport Traffic Control Towers (ATCTs), Automated Flight Service Stations (AFSSs), Backup Emergency Communications (BUECs), Remote Communications Air/Ground Facilities (RCAGs), Automated Weather Observing Stations (AWOSs), and Air Route Surveillance Radars (ARSRs). Architectures that integrate voice and data (both operational and administrative) were developed and evaluated.

1.2 OBJECTIVES AND SCOPE OF THE STUDY

In the previous efforts, a complete set of network requirements was developed, and the feasibility of synthesizing a network with Commercial Off The Shelf (COTS) components that will meet these requirements was explored. The objectives of this Task 11 study were to determine how such a specified service could be expected to perform (and at what cost), how selected systems might be transitioned and converted to the new communications architecture, and to explore special topics that have a high degree of relevance to these issues. Some of the specific issues this study addressed were:

- Support of Domain Name Services (DNS) and Network Directory Services (NDS), and network service assurance.
- What protocols should be supported? How does the FAA convert legacy data to these protocols? How does the FAA ensure that a robust, cohesive, naming and addressing policy is developed and followed by all program offices and facilities?
- How does the FAA transition from the leased circuit connectivity model that describes the NAS communications architecture of the present to the amorphous cloud that is the model for packet switched networks? What services should be migrated first?
- Given the basic set of Quality of Service (QoS) requirements of latency, integrity, and availability for each of the traffic categories, what degree of insight into the service provider network is required to ensure that these requirements are being met?

The scope of this task included the development of a representative architecture based on modern telecommunications technologies for a subset of the Cleveland (ZOB) ARTCC. The intent was to evaluate this architecture, and demonstrate that FAA requirements for operational voice and data, as well as administrative voice and data could be served by these technologies at reasonable cost.

Furthermore, issues associated with the transitioning to this architecture were to be specified. A specific set of protocols and implementation techniques were to be recommended.

1.3 ORGANIZATION OF THIS REPORT

This report includes six sections and four appendices:

- Introduction
- Key Technology, Protocols, and Standards for Supporting Services
- Comparative Analysis of FAA Communications Service Needs vs. Available Services and Technologies
- Application of Available Services/Technologies to ZOB
- Evaluation of the ZOB Architecture
- Conclusions and Recommendations
- Appendix A: FAA Telecommunication Service Criticalities and Diversity Priorities

- Appendix B: Node Diagrams for Baseline, Scenario 1A, Scenario 1B and Scenario 2 Architectures
- Appendix C: Architecture Circuit Lists
- Appendix D: Latency and Availability Calculations

This section is the Introduction, and describes the scope of this study, placing it in the context of the FAA telecommunications problem and previous studies.

Section 2 discusses the key telecommunications technologies that enable an integrated services network carrying mission critical data and administrative data to perform to specification. These technologies include:

- The protocols that have been developed to provision and provide for QoS.
- The protocols that have been developed to provide for information security.
- The protocols that have been developed to provide for transmission of voice and video over fast packet networks.
- The standards that have been developed to provide for effective enterprise management.

Section 3 discusses the service needs of the FAA and compares them with the performance of current commercial wide area network services and technologies. This comparison is discussed in four categories as follows:

- Data Delivery Service
- Voice and Videoconferencing
- Security
- Enterprise Management

Section 4 outlines the methodology and results of the process used to describe commercial backbone network architectures and services; identifies a subset of FAA sites to analyze; determines communication requirements of the FAA sites; and specifies the connection to, and use of, commercial networks to satisfy FAA communication requirements.

Section 5 provides a performance assessment of the developed architecture. This performance is described and evaluated in terms of cost, availability, and latency performance of the architecture. Additionally, Section 5 provides specific transition issues associated with migrating the Voice Switching and Control System (VSCS) to a Voice over Internet Protocol (VoIP) architecture.

Section 6 provides the conclusions and recommendations that were generated by this study.

1.4 LIST OF DOCUMENTS

Numerous documents were used in the preparation of this report. Source material is noted by the use of endnotes. The following abbreviated list provides some of the more important source documents that were used in the preparation of this report.

Traffic Flow Management Communications Architecture Study, Stanford Telecom TR97052, 29 May 1997.

NAS Communications Concept Of The Future Final Technical Report, June 1997, Federal Systems Integration And Management Center Federal Systems Integration Center (FEDSIM), Subtask 036 of contract 90070TND-02.

NAS Router Case File, March 1994, Federal Systems Integration And Management Center Federal Systems Integration Center (FEDSIM), Subtask 019-5 of contract GS-00K-92AJC1006.

Washington DC ARTCC to New York ARTCC Asynchronous Transfer Mode (ATM) Analysis Final Technical Report, September 1997, Federal Systems Integration And Management Center Federal Systems Integration Center (FEDSIM), Subtask 41-1 of contract 90070TND-02.

International Vocoder Placement and Air/Ground Circuit Compatibility Assessment, March 1996, Federal Systems Integration And Management Center Federal Systems Integration Center (FEDSIM), Subtask 029-3 of contract 90070TND-02.

A/G Communications Architecture, FEDSIM Subtask 38-4 of contract 90070TND-02, Final Report, July 1997.

Air Traffic Management Communications Architecture Study, Stanford Telecom TR97052, 15 September 1997.

ATM Communications Transition and Implementation Plan, Volume 1: Evaluation of Alternatives, Stanford Telecom TR98031, February 1998.

ATM Communications Transition and Implementation Plan, Volume 2: ETMS Communications Network Transition Plan, Stanford Telecom TR98031, February 1998.

NAS Communications Architecture – Design Alternatives, Stanford Telecom TR98083, November 1998.

En Route Surveillance Architecture and Tracking Study, Stanford Telecom TR99009, May 1999.

Automation System Communications Requirements, Stanford Telecom TR99004, May 1999.

National Airspace System Architecture, Version 4.0, US Department of Transportation, Federal Aviation Administration, January 1999.

Federal Aviation Administration (FAA) Telecommunications Infrastructure (FTI) Technical Guidance Document, August 23, 1999.

Current FAA Telecommunications System and Facility Description Manual, Currant Book, Fiscal Year 1999 Edition, NAS Operations (AOP) Telecommunications Support and International Communications Division, AOP-600.

Future FAA Telecommunications Plan, "Fuchsia Book", NAS Operations (AOP) Telecommunications Network Planning and Engineering Division, April 2000.

Federal Aviation Administration Telecommunications Infrastructure, Mission Need Statement Number 322, January 30, 1998.

FAA Telecommunications Infrastructure Investment Analysis Report, July 13, 1999.

Information System Security Architecture, Version 1.0, FAA ASD, March 30, 2000.

2. KEY TECHNOLOGY, PROTOCOLS, AND STANDARDS FOR SUPPORTING SERVICES

2.1 TECHNOLOGY, PROTOCOLS, AND STANDARDS FOR QOS PROVISIONING

Quality of Service (QoS) is defined by the International Telecommunication Union (ITU) Transmission Systems and Media (ITU-T) (previous the Consultative Committee on International Telephony and Telegraphy (CCITT)) in Recommendation E.800 as: *"The collective effect of service performance which determines the degree of satisfaction of a user of the service."* For point-to-point circuit communications, the provision of QoS is a comparatively simple matter since, in circuit communications, a defined set of resources of the circuit-switched network are dedicated to the service support. Thus, provisioning a specified QoS for circuit service is accomplished simply by provisioning the dedicated resources that support that service with the required quality. In a packet network, however, network resources are entirely shared so making a QoS guarantee is much more complicated.

In general, QoS may include a large number of performance parameters, but in the context of this report, the focus of QoS is on parameters of:

- Bandwidth
- Availability
- Data delay /data delay jitter
- Packet data loss

How a QoS in a packet network may be guaranteed is discussed in the following subsections, but Table 2.1-1 provides an overview of the basic tools.

The QoS offered by a communications network service provider is typically the subject of a Service Level Agreement (SLA) that provides a guarantee of performance for a designated data service. Provision for requesting and assuring a QoS requires:

- A “signaling” protocol through which the user requests a defined QoS level.
- Traffic routing and management protocols used by the service provider to assure the requested QoS level is met.

Example QoS offerings supported by alternative networks include the following:

- Best effort service as offered with plain Internet (IP) Network – no congestion management in place to address traffic peak loads or failures.

- Constant bit rate (CBR) service as offered in Asynchronous Transfer Mode (ATM) service - specifies peak cell rate (PCR), cell delay variation tolerance (CDVT), and cell loss rate (CLR).

Table 2.1-1: Tools for Guaranteeing Key QoS Parameters

QoS Parameter	Tools for Supporting
Bandwidth	Bandwidth is guaranteed via a number of bandwidth reservation protocols that dedicate switching and bandwidth to a data stream within the shared network environment. Reservation alternatives include: <ul style="list-style-type: none"> • On demand: Switched Virtual Circuits (SVC), Resource Reservation Protocol (RSVP) • Pre-arranged: Permanent Virtual Circuit (PVC)
Availability	High Availability is achieved via redundant and self-healing networks. <ul style="list-style-type: none"> • Synchronous Optical Network (SONET) Layer redundancy • Rerouting in response to failure • Redundant access links to network backbone
Data Delay / Data Delay Jitter	Low Data Delay and Delay Jitter is achieved by: <ul style="list-style-type: none"> • Congestion detection and traffic management • Traffic shaping • Priority switching
Packet Loss	Low percentage Packet Loss is provided by: <ul style="list-style-type: none"> • Low SONET Bit Error Rate ($< 10^{-9}$) • Plus, all of the methods above that control delay also assure that congestion is avoided so that packet loss due to network congestion is avoided.

Class of Service (CoS) and Type of Service (ToS) are two terms that are often used in the context of QoS discussion. Usually CoS and ToS are equivalent terms. In a packet switched network, CoS/ToS is the ability of switches and routers to prioritize traffic into different queues or classes. CoS/ToS (by itself) does not guarantee a QoS in a packet network. Without other measures, CoS/ToS supports only a “best effort” service, although the highest class will get the best service in a network of mixed services. IPv4 supports CoS/ToS via the ToS byte in the packet header.

In general, provision of QoS requires CoS/ToS plus a number of additional measures such as:

- Protocols through which the user service requests are reviewed: e.g., admission control policies and traffic management protocols used by the service provider, including queuing mechanisms and congestion management at routers.
- Deterministic path selection algorithms and other mechanisms based on latency, jitter and other path metrics.
- Collection of metrics to assure that a specified QoS level is met.

IPv6 supports QoS.

2.1.1 Provision for Bandwidth Reservation

In a packet network, bandwidth may be reserved by setting up a virtual circuit that reserves a set of channel and switching resources for specified services. Reservations may be static (pre-arranged), or may be dynamically arranged on demand via a user request.

2.1.1.1 Static Reservation

Pre-arranged virtual circuits are typically referred to as Permanent Virtual Circuits (PVCs). PVCs are set up by a network operator via a network management system, and there is a fixed lead time for installation of a PVC. PVCs are defined as connections between two sites or endpoints. They are fixed path, and are not available on demand or on a call-by-call basis. PVCs are supported by common network service protocols.

2.1.1.2 Dynamic Reservation

Reservation of bandwidth on demand is achieved by setting up a Switched Virtual Circuit (SVC). SVCs are available on a call-by-call basis, and are established by using the SVC signaling protocol (Q.933). In setting up an SVC, a user specifies a destination address similar to a phone number. Both Frame Relay and ATM services support SVCs. At the IP layer, SVC type services are supported via the Resource ReSerVation Protocol (RSVP). RSVP is a standard that was developed by the IP Integrated Services Working Group (IntServ). The RSVP Version 1 Functional Specification is documented in Request For Comment (RFC) 2205. RSVP allows sender/receivers to set up reservations of network resources (at each hop) for both unicast and multicast data streams. The network orchestrates several processes that support this service:

- **Policy Control** - Determines if the user has rights to make a reservation.
- **Admission Control** - Keeps track of available network resources.
- **Packet Classifier** - Determines QoS of each packet (e.g., which queue).
- **Packet Scheduler** - Distributes system resources among flows (e.g., queue manager), measures properties of flows, and determines policies where needed.

RSVP uses emerging switching protocols such as Multi-Protocol Label Switching (MPLS) for resource reservation, virtual channels, and packet prioritization.

2.1.2 Provision for High Availability

High availability of the backbones of modern packet communications networks is achieved via a number of redundancies in all layers of the communications protocol stack. Several layers of a communications protocol stack are illustrated in Figure 2.1-1. In general, the redundancy supports a “self-healing” behavior of the networks so that link failures are rapidly detected and restored.

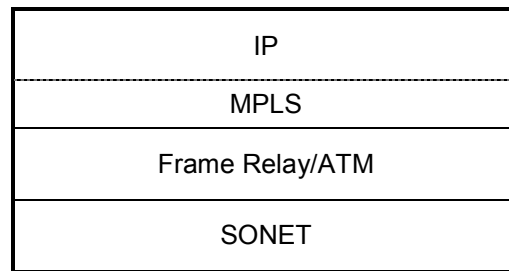


Figure 2.1-1: Example Communications Protocol Stack

2.1.2.1 Physical Layer Redundancy

Most Wide Area Network (WAN) communications networks are built upon a Synchronous Optical Network (SONET) physical layer, where there is a built in redundancy of the optical fiber. SONET data rates are based upon a Synchronous Digital Hierarchy supporting data rates in Digital Signal 3 (DS3) multiples of 3, 12, 48, 192. OC-192, for example, supports a data rate of 10 Gbps. Most modern SONET implementations have a built in redundancy as illustrated in Figure 2.1-2. This figure shows a 4-Fiber Bi-directional Line Switched Ring (4F-BLSR) that is rapidly self-healing (cuts are restored in < 1 msec). The four fibers of a 4F-BLSR consist of a “working” pair and a “protect” pair. If the working pair is cut, traffic that was on the cut working pair is routed in opposite direction via the protected pair *with no loss in capacity*. For this reason, most service providers are building networks over 4F-BLSR in order to provide a high network availability.

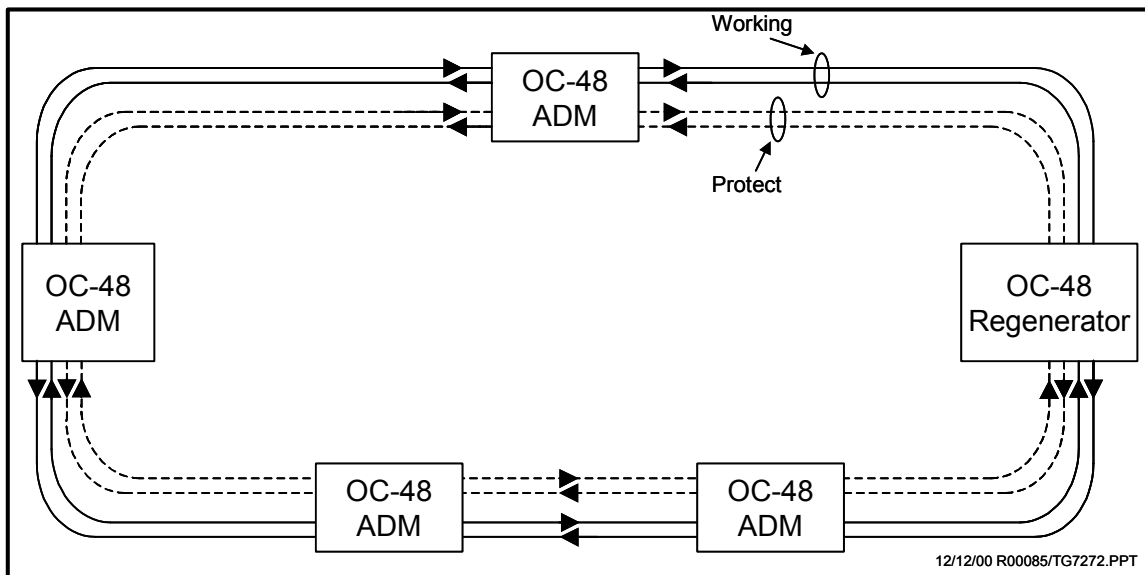


Figure 2.1-2: SONET 4 Fiber Bi-directional Line Switched Ring (4F-BLSR)

2.1.2.2 Network Layer Redundancy

Above the physical layer there are other mechanisms that promote the self-healing of the network. At the network layer, routes are automatically reconfigured in response to node/line failure. The timeframe for such rerouting healing varies depending upon the route discovery protocols that are utilized:

- Rerouting can be slow: tens of seconds with Routing Information Protocol (RIP), Interior Gateway Routing Protocol (IGRP) algorithms.
- Rerouting can be fast: few seconds or less with Open Shortest Path First (OSPF), Enhanced IGRP algorithms.
- Rerouting can be very fast: 50 msec claimed with MPLS.

2.1.2.3 Network Robustness During Failures

Re-routing protocols in combination with the redundancy afforded by 4F-BLSR on the WAN establish near 100% availability for backbone communications services. As illustrated in Figure 2.1-3, communications connectivity between the points B and C is maintained even with a double failure. With a single failure (cut at segment “e”), there is no impact on the capacity. With a double failure (cuts at “e” and “c”), the capacity is reduced, but the connectivity is maintained. Thus, in a network carrying a number of different priority communications, the most critical communications would be favored and therefore unaffected even with double failures. By such techniques at these, network backbones have achieved a demonstrated availability of 0.99999 and greater.

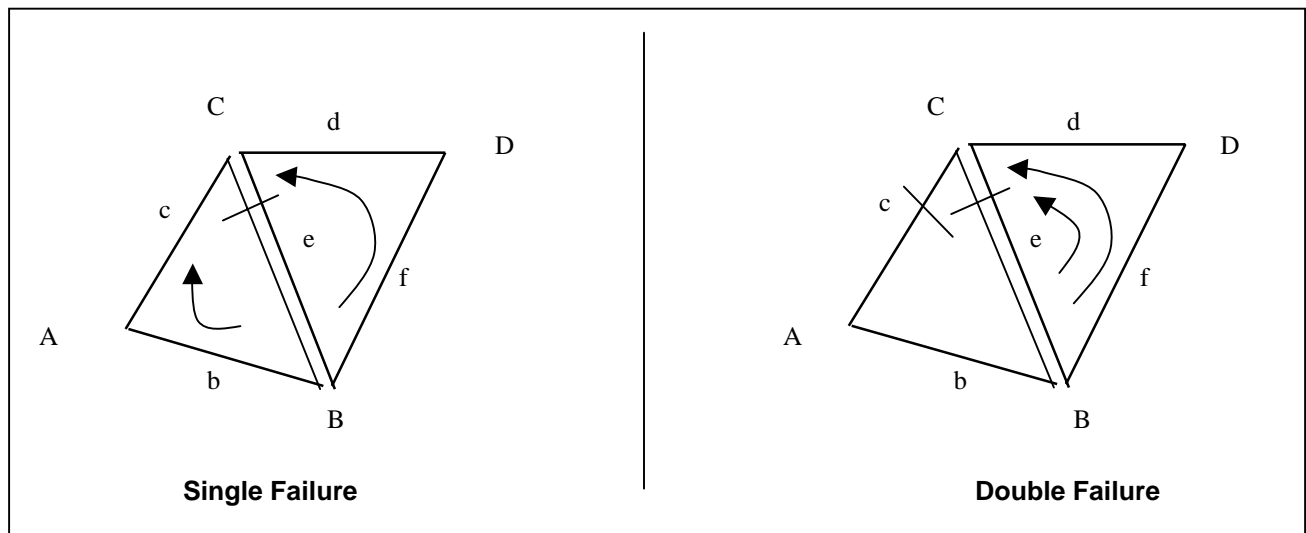


Figure 2.1-3: Robustness of Backbone Communications Between Points B and C

2.1.3 Provision for Low Data Delay and Delay Jitter

Because packet communications networks share bandwidth, the time delay of a packet through a packet network is not deterministic. In general, the delay of a packet through a network depends upon the amount of congestion in the network and the nature (e.g., packet sizes and priorities) of other traffic. Controlling the delay in a packet network is thus a primary challenge in offering QoS over a packet network. IP Differentiated Services Working Group (DiffServ) has developed an approach to address this via a simple use of a ToS byte in an IP packet to determine alternative per hop behavior (PHB). This approach does not require any setup protocol (i.e., accessing DiffServ does not explicitly signal the network router before sending data) and it involves only the sender and the network. The sender sets the packet priority via a ToS byte and the network routes the sent packet with a PHB associated with the ToS byte of the packet. In addition to DiffServ, a variety of Network Traffic Management Protocols augment and support the ability of DiffServ to provide different QoS levels for data delay on a common network. These include protocols for:

- Congestion management: First In First Out (FIFO) queuing, priority queuing (PQ), weighted fair queuing (WFQ).
- Congestion avoidance: random early detection (RED), weighted RED (WRED).
- Traffic policing: network approval/denial for bandwidth above a critical amount.
- Traffic shaping: e.g., requiring smaller packet sizes for traffic, which decreases overall delay jitter.

2.1.4 Provision for High Probability of Packet Delivery

The primary factors that can result in lost packets are bit errors (which may cause packets to become corrupted, and congestion (which may cause some packets to be dropped by a router). The very low bit error rate (BER) of a SONET connection ensures packet loss will be very low due to BER. SONET delivers a $BER < 10^{-9}$. Packet loss due to congestion at routers is made small by managing the network with measures such as congestion avoidance, bandwidth reservation, and priority routing for critical data streams that have the least tolerance to packet loss.

2.2 TECHNOLOGY, PROTOCOLS, AND STANDARDS FOR INFORMATION SECURITY

2.2.1 Need For Security

Security is a critical issue affecting data communications networks. Modern data networks need to be protected from at least the following common attacks³:

- Tapping the wire: to gain access to cleartext data and passwords.
- Impersonation: to get unauthorized access to data or to create unauthorized emails, orders, etc.
- Denial-of-service: to render network resources non-functional.
- Replay of messages: to get access to and change information in transit.

- Guessing of passwords: to get access to information and services that would normally be denied.
- Guessing of keys: to get access to encrypted data and passwords (brute-force attack, chosen ciphertext attack, chosen plaintext attack).
- Viruses, trojan horses, and logic bombs: to destroy data.

The consequences of a security-compromised National Airspace System (NAS) system could range from the merely annoying to the catastrophic. The need for security on Federal networks is mandated by Federal law, specifically, the Computer Security Act of 1987. This section describes modern network security technologies, protocols, and standards. How Federal security requirements affect the Federal Aviation Administration (FAA), its response, and how security technology should be applied to FAA NAS communications systems will be discussed in Section 3.3.

2.2.2 Security Solutions

Given the common types of security attacks mentioned above, there are a host of generic security solutions that may be employed, including the following⁴:

- Encryption: to protect data and passwords.
- Authentication and authorization: to prevent improper access.
- Integrity checking and message authentication codes (MACS): to protect against the improper alteration of messages.
- Non-repudiation: to make sure that an action cannot be denied by the person who performed it.
- Digital signatures and certificates: to ascertain a party's identity.
- One-time passwords and two-way random number handshakes: to mutually authenticate parties of a conversation.
- Frequent key refresh, strong keys, and prevention of deriving future keys: to protect against breaking of keys (crypto-analysis).
- Address concealment: to protect against denial-of-service attacks.
- Content inspection: to check application level data for malicious content before delivering it into the secure network.

There are numerous methods to implement these security solutions in a computer network, many of which can be applied in combination. These methods need to be selected by performing tradeoffs among desired level of security versus user impacts versus cost. Several common protocols and systems are employed in most modern computer networks, particularly in Transport Control Protocol (TCP)/IP networks. These include the following:

- IP filtering
- Network Address Translation (NAT)

- IP Security Architecture (IPSec)
- SOCKS (SOCK-et-S, an internal NEC development name)
- Secure Sockets Layer (SSL)
- Application proxies
- Firewalls
- Kerberos, Remote Authentication Dial-In User Service (RADIUS), and other authentication systems

Where these specific solutions fit within the TCP/IP layers is shown in Figure 2.2-1 below.

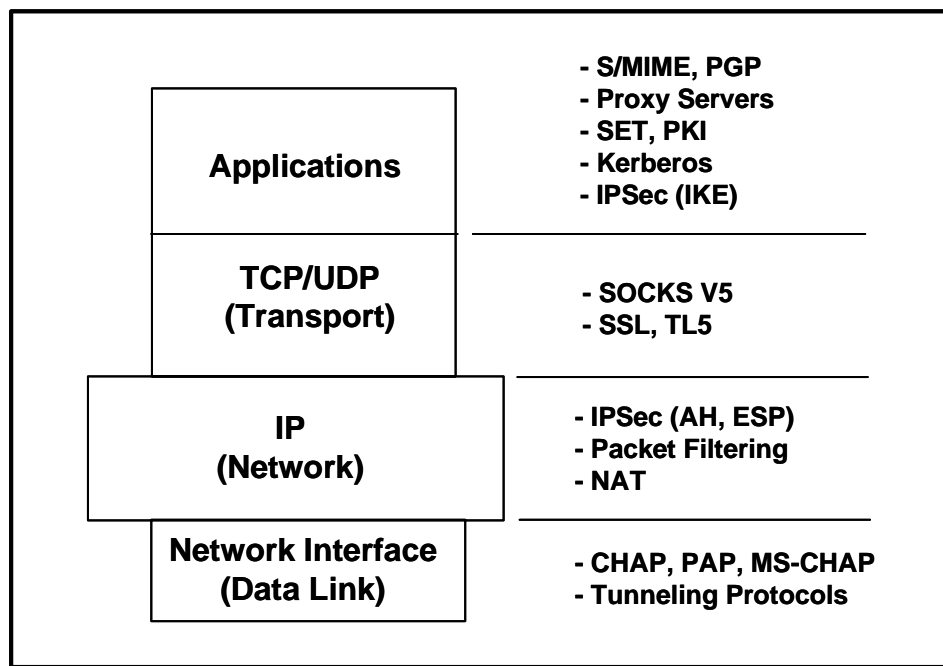


Figure 2.2-1: Security Solutions in the TCP/IP Layers

Many of the security protocols/standards shown in the different layers in the figure feature encryption and/or authentication as part of their solutions; however, there are relative advantages/disadvantages to providing these functions in the different layers:

- **Application/Transport Layer** – A mechanism such as SSL provides data privacy for each application individually but does not protect data between two different applications. That is to say, every system and application must be protected with SSL in order for it to work efficiently.
- **Network Layer** – IPSec is a standard framework for end-to-end secure communications at the IP network level. Thus it is transparent to the applications like Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), Telnet, etc. It is mandated in Internet Protocol Specification Version 6 (IPv6) and an option in Internet Protocol Specification Version 4 (IPv4).

- **Data Link Layer** – With link level encryption, both ends of the communication link are protected by encryption devices. This method provides excellent protection of data as long as the data is on the link, but at the end of the links the data is in a clear text form and thus insecure. Also, as the number of the communication links increases the manageability of the network becomes difficult.

Providing security at the network layer with a protocol such as IPSec offers the advantages of flexibility combined with high performance. For these and other reasons, IPSec has become the IP standard. IPSec is discussed in greater detail in the next section.

2.2.3 IPSec

IPSec is based on modern cryptography techniques and provides very strong data authentication and privacy guarantees. Besides being transparent to TCP/IP applications, it offers the following other advantages:

- It is independent of network topologies and therefore works well with Ethernet, Token Ring and Point to Point Protocol (PPP).
- Unlike vendor initiated tunneling protocols like Point to Point Tunneling Protocol (PPTP), Layer 2 Tunneling Protocol (L2TP) and Layer 2 Forwarding Protocol (L2F), IPSec provides standard-based tunneling, authentication and encryption.
- IPSec can be used for any number of protocols in a tunneling mode.

2.2.3.1 IPSec Architecture

Figure 2.2-2 shows the IPSec architecture, as delineated in Internet Engineering Task Force (IETF) Request for Comments (RFC) 1825. As shown in the figure, it consists of the following three components:

- **Authentication Header (AH)** – Used to verify the sender's identity, packet's content, and data integrity.
- **Encapsulating Security Payload (ESP)** – Provides support for privacy/confidentiality, data integrity and authentication. It can be used to encrypt either: 1) a transport layer segment (transport mode ESP), or 2) an entire IP packet (tunnel mode ESP).
- **Key Management** – the Key management protocol negotiates the security association. It is a method that describes how the two peers will use security services (encryption and authentication) for secure communication, including manual key exchange, Simple Key Interchange Protocol (SKIP), or Internet Key Exchange (IKE). IETF chose IKE as the standard framework for security attributes.

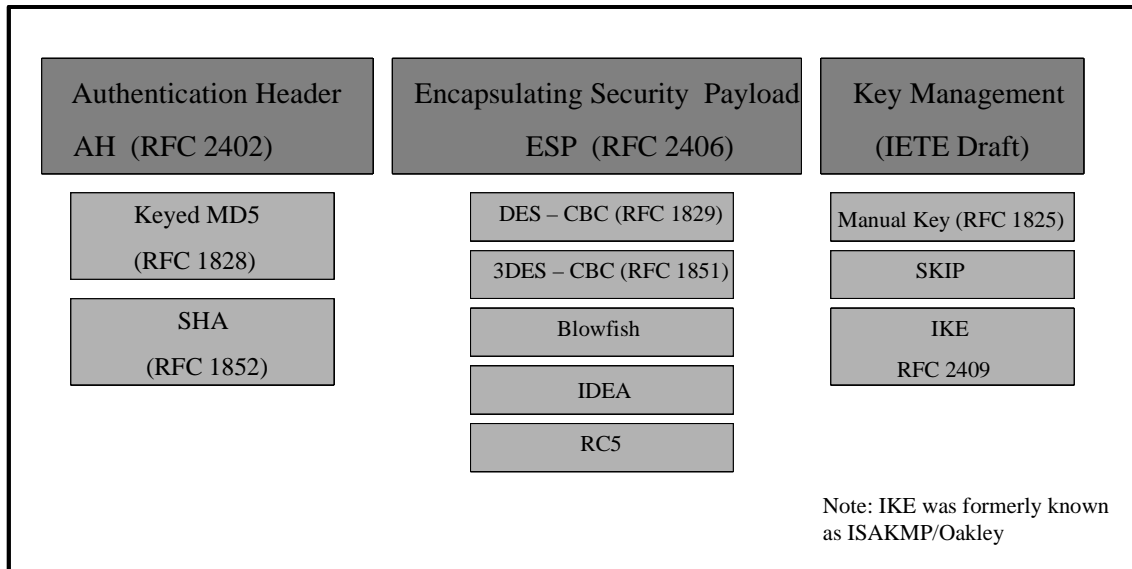


Figure 2.2-2: IPsec Security Architecture (RFC 1825)

2.2.3.2 IPsec Authentication

Authentication, that is, ensuring proof of identity of the user, is essential to safeguard a communications system from an intruder and it is often achieved through following methods:

- **Challenge and Response:** This is the most common form of security achieved through a user's login Identification (ID) and password. In this case the passwords have to be carefully chosen and maintained.
- **Digital Certificates:** A digital certificate, issued by a trusted certificate authority (CA), authenticates the sender's identity to the receiver by providing a digitally signed sender's public key. Both the sender and the receiver have a CA certificate and so, without contacting the third party, this method can authenticate the messages in both directions.
- **Message digest and digital signature:** Instead of encrypting the data itself, a one-way hash function of the data, such as RSA Message Digest 5 Algorithm (MD5) or Secure Hashing Algorithm (SHA), is calculated (called the Message Digest). The message digest is encrypted using the sender's private key.
- **Using a Pre-shared Key:** This method uses symmetric keys previously installed on each host. When one of the hosts sends a keyed hash of data including his pre-shared key, the second party is independently able to create the same hash value using its pre-shared key.

2.2.3.2.1 IPsec Authentication Headers

There are many transforms (algorithms) specified for header authentication. The two most common transforms are:

- **Keyed MD5:** The MD5 message digest algorithm takes as its input a message of arbitrary length and produces as its output a 128-bit message digest. The input is processed in 512-bit blocks. The MD5 algorithm is performed over the following sequence: Key, Keyfill, IP packet, Key, MD5fill,

where Key is the secret key. Keyfill is padding so that key concatenated with keyfill is equal to integer multiples of 512-bits, IP packet is the IP packet with appropriate fields set to zero, and MD5fill is the padding supplied by MD5.

- **SHA:** This algorithm takes a message of less than 2^{64} bits in length and produces a 160-bit message digest. The algorithm is slightly slower than MD5, but the larger message digest makes it more secure against brute force collision and inversion attacks.

2.2.3.3 IPSec ESP

2.2.3.3.1 Encryption in ESP

IPSec ESP keeps transmitted information strictly confidential by fully encrypting the data, or payload, in all packets. This prevents other users from “listening in” to the open exchange of information. Several generic encryption schemes provide candidates for implementing ESP:

- **Shared Key Encryption or Symmetric key Encryption:** With this system both parties share the same key for encryption and decryption. The use of a symmetric key is efficient as it decreases the time delay for encryption and decryption, and provides a degree of authentication as the information encrypted by a symmetric key can only be decrypted by the same key. Shared key encryption systems use Data Encryption Standard (DES), Triple Data Encryption Standard (3DES), RSA Rivest Cipher 5 Algorithm (RC5) and International Data Encryption Algorithm (IDEA) algorithms. The weakness is if the key becomes known, there is a loss of both privacy and authenticity.
- **Public Key Encryption or Asymmetric Encryption:** This system involves a pair of keys – Public Key and Private key. The private key is kept secret (known only to the sender) and the public key, is used by the receiver. Public key encryption can also be used to transfer a symmetric key. Public key encryption is very Central Processing Unit (CPU) intensive and so it is typically used for small amount of data where strong security is required. There are two ways to use this system:
 - Using the receiver’s public key to encrypt: In this case, the secret key is only possessed by the receiver so he is the only one who can decrypt the data. The disadvantage is that the authenticity of the sender cannot be guaranteed.
 - Using the sender’s private key to encrypt: In this case a digest of the original message, using hash algorithms, is created and encrypted with the sender’s private key. The result of this method provides data privacy, authenticity, and non-repudiation.
- **Secure Key Exchange:** In this scenario, both users, sender and receiver, first authenticate themselves during a session-specific encryption key distribution process. The session key is created based on data generated by both parties at the time of communication. This key can then be used to encrypt and decrypt all other communications.

2.2.3.3.2 IPSec Transport Mode and Tunnel Mode ESP

As described above, in IPSec encryption can be performed in two different modes: transport mode and tunnel mode. Each has its advantages and disadvantages. These are listed in Table 2.2-1.

Table 2.2-1: Relative Advantages and Disadvantages of Transport Mode Versus Tunnel Mode

	Transport Mode	Tunnel Mode
Advantages	<p>Adds only a few bytes to each packet as no new IP header or IP extension headers are added.</p> <p>Since the final source and the destination address of the packet are visible to the devices on the common network, special processing, like ToS byte priority routing, can be enabled in the intermediate network.</p> <p>Since the IP address provided is of the final destination, transport mode provides host-to-host connection.</p>	<p>The entire original IP datagram is encrypted and thus makes traffic analysis a difficult process.</p> <p>In this mode the router does the encryption/decryption and thus takes off the load from the host.</p> <p>With IPSec tunnel mode deployed in the network, none of the operating systems or any applications on the PCs or servers have to be modified.</p>
Disadvantages	<p>As the IP header is in clear text in the transport mode, traffic analysis can be performed on the packets.</p> <p>As the tunnel is passing the firewall/router, hacker can follow the same path and enter the network.</p> <p>Since encryption and authentication is performed at the host system, this increases the load on the host whereby the processing speed decreases.</p> <p>Since there are many more hosts than tunnels, security management is far more complex in the transport mode.</p>	<p>With the addition of a new IP header in the tunnel mode, the size of the packet and the processing burden increases.</p>

From the table one can conclude that IPSec tunnel mode is better for transition, entails simpler security management, and provides a more secure connection than IPSec transport mode. This makes it an ideal candidate for Virtual Private Networks (VPNs) (see Section 2.3.4 below).

2.2.3.4 IPSec Key Management

As described above, Key Management is the method for determining how two peers will use security services (encryption and authentication) for secure communication. The integrity of these security services is highly dependent on getting the keys to authorized users (key exchange) and keeping the keys out of the hands of unauthorized users. The three most common methods for key exchange include the following:

- **Manual Key Exchange:** Here the configuration of the keys for all the systems is done manually. As long as the network size is small and static, manual key exchange is quite practical, but the job becomes tedious and impractical as the network grows.
- **SKIP:** This key management system was proposed by Sun Microsystems but its failure to be approved by the IETF has restricted its commercial implementation to Sun and its partners.
- **IKE:** IKE, formerly known as ISAKMP/Oakley (Internet Security Association and Key Management Protocol/Oakley Key determination Protocol), has been formally chosen as a standard for IPv6 by IETF and as an option for IPv4. IKE provides a framework for Internet Key Management, provides specific protocol support for negotiations, and establishes a shared session key in order to encrypt the IKE tunnel.

2.2.4 Virtual Private Networks

As businesses and government agencies increasingly turn towards the Internet, commercial WANs, and other “untrusted” networks to provide network connectivity between their own distributed internal, “trusted” networks, they have come to rely on VPNs to provide a high level of security.

A VPN is a distributed private network that makes use of a common telecommunication infrastructure for communication, maintaining privacy through tunneling protocols or security associations. VPN advantages include the following:

- Network traffic from many sources can travel via separate tunnels across the same infrastructure.
- Network protocols can traverse incompatible infrastructures through encapsulation techniques.
- Traffic from many sources can be differentiated, so that the traffic can be routed to specific destinations and receive specific levels of service.

Figure 2.2-3 provides an overview of VPN topology.

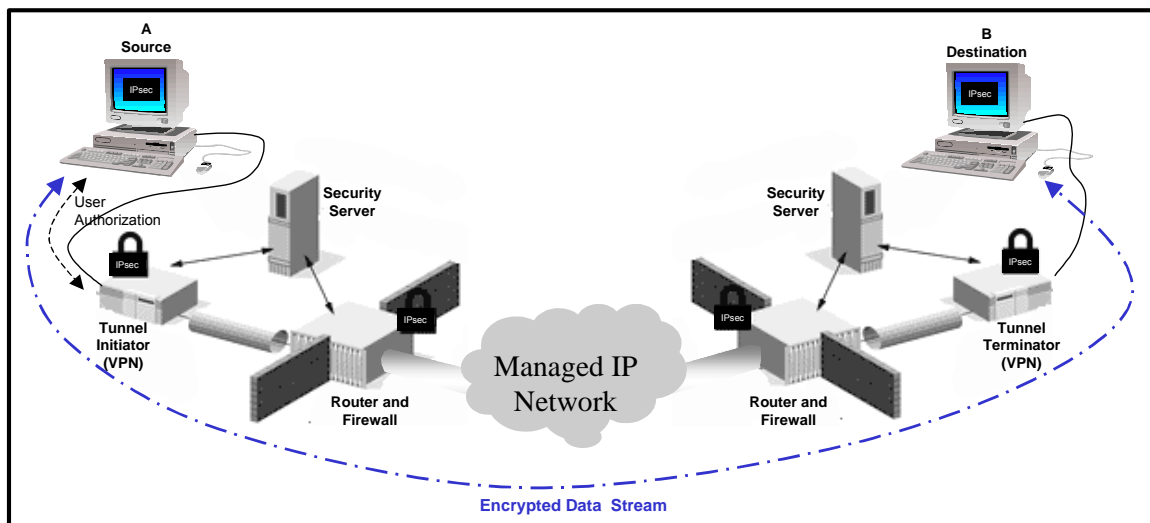


Figure 2.2-3: VPN Topology

The basic components of a VPN tunnel are:

- A Tunnel Initiator (TI)
- A Routed Network
- A Tunnel Terminator (TT)

A VPN is defined between a tunnel initiator and a tunnel terminator. The VPN process can be summarized as follows:

- The Tunnel Initiator first encapsulates the original data packet within a new packet, called a tunnel packet, with a new source and destination address. Encapsulation provides a way for a non-IP packet to travel over an IP network through tunneling. The tunnel packets are all IP based packets, so the encapsulated packets can be of any protocol.
- The tunnel terminator reverses the encapsulation process, strips off the new headers, and passes the original packet to a local protocol stack or the local network at the destination.

VPNs offer a host of security features that work together to provide excellent security over an untrusted network. These features include the following:

- **Confidentiality:** Confidentiality can be provided by “encrypting” the encapsulated data. Both the TI and the TT share the encryption scheme. DES, 3DES, IDEA, Rivest, Shamir, Adleman Algorithm (RSA), RSA Rivest Cipher 4 Algorithm (RC4) and RC5 are some of the common standards encryption algorithms supported. For decrypting the data the provision for key exchange is provided by IKE.
- **Authentication:** the end points, TI and TT, are authenticated. Token-based, NT Domains, UNIX password, RADIUS and X.509 are some of the authentication services available.
- **Data Integrity:** The integrity of the tunneled data is assured with algorithms like the message digest or hash function.
- **Access Control:** Access control systems are generally implemented using firewalls, which provide a centralized point from which to permit or deny access. Packet-filtering firewalls and application/proxy firewalls are available with integrated VPN support in them.
- **Event Logging:** In order to manage and audit a network, an event log is required. This log should automatically record important events such as adding or deleting a user, and session start and end data. NAT/IP Port Translation (PAT), Dynamic Host Configuration Protocol (DHCP), intrusion detection, and security logging are some of the network services supported with VPNs.
- **Tunneling:** Tunneling encapsulates the payload, regardless of its format, within a standard internet “envelope” in order to protect it from viewing by an unauthorized user. PPTP, L2F, L2TP and IPSec are the most common protocols used for tunneling.

IPSec is a favored protocol for tunneling because of the three interlocking technologies (AH, ESP, and IKE) that combine to defeat the traditional threats to IP-based networks. A VPN device implementing IPSec is called a security gateway. As mentioned above, the IPSec tunneling mode ESP is the preferred mode of operation because it requires that only the security gateway be IPSec “aware,” whereas the transport mode requires all end users to have unique IP addresses to be IPSec aware. Figure 2.2-4 illustrates encapsulation in the IPSec tunneling mode ESP.

Tunnel IP Header	IPSec Header	User IP Header (encrypted)	Upper level protocols & data (encrypted)
------------------	--------------	-------------------------------	---------------------------------------------

Figure 2.2-4: Encapsulation in the IPSec Tunneling Mode ESP

2.2.5 VPN Access Control - Firewalls

Up to this point, the VPN discussion has focused on the means to protect user data, such as authentication and encryption. Access control is another important aspect of VPN security features, and firewalls are the principal means of controlling access between a trusted network and a less trusted one. A firewall is not a single component, but rather a strategy for protecting an organization's networked resources.

Firewalls provide several types of protection⁵:

- They can block unwanted traffic.
- They can direct incoming traffic to more trustworthy internal systems.
- They hide vulnerable systems that can not easily be secured from the Internet.
- They can log traffic to and from the private network.
- They can hide information like system names, network topology, network device types, and internal user ID's from the Internet.
- They can provide more robust authentication than standard applications might be able to do.

As with any safeguard, there are trade-offs between convenience and security. Transparency is the visibility of the firewall to both inside users and outsiders going through a firewall. A firewall is transparent to users if they do not notice or stop at the firewall in order to access a network. Firewalls are typically configured to be transparent to internal network users (while going outside the firewall); on the other hand, firewalls are configured to be non-transparent for outside network coming through the firewall. This generally provides the highest level of security without placing an undue burden on internal users.

2.2.5.1 Types of Firewalls⁶

There are different implementations of firewalls that can be arranged in different ways. The various firewall implementations are discussed below.

2.2.5.1.1 Packet Filtering Gateways

Packet filtering firewalls use routers with packet filtering rules to grant or deny access based on source address, destination address, and port. They offer minimum security but at a very low cost, and can be an appropriate choice for a low risk environment. They are fast, flexible, and transparent. Filtering rules are not often easily maintained on a router, but there are tools available to simplify the tasks of creating and maintaining the rules.

Filtering gateways do have inherent risks including:

- The source and destination addresses and ports contained in the IP packet header are the only information that is available to the router in making decision whether or not to permit traffic access to an internal network.
- They do not protect against IP or Domain Naming System (DNS) address spoofing.
- An attacker will have a direct access to any host on the internal network once access has been granted by the firewall.
- Strong user authentication is not supported with some packet filtering gateways.
- They provide little or no useful logging.

2.2.5.1.2 Application Gateways

An application gateway uses server programs (called proxies) that run on the firewall. These proxies take external requests, examine them, and forward legitimate requests to the internal host that provides the appropriate service. Application gateways can support functions such as user authentication and logging.

Because an application gateway is considered as the most secure type of firewall, this configuration provides a number of advantages to the medium-high risk site:

- The firewall can be configured as the only host address that is visible to the outside network, requiring all connections to and from the internal network to go through the firewall.
- The use of proxies for different services prevents direct access to services on the internal network, protecting the enterprise against insecure or misconfigured internal hosts.
- Strong user authentication can be enforced with application gateways.
- Proxies can provide detailed logging at the application level.

Application level firewalls should be configured such that out-bound network traffic appears as if the traffic had originated from the firewall (i.e. only the firewall is visible to outside networks). In this manner, direct access to network services on the internal network is not allowed. All incoming requests for different network services such as Telnet, FTP, HTTP, etc., regardless of which host on the internal network will be the final destination, must go through the appropriate proxy on the firewall.

Applications gateways require a proxy for each service, such as FTP, HTTP, etc., to be supported through the firewall. When a service is required that is not supported by a proxy, an organization has three choices:

- Deny the service until the firewall vendor has developed a secure proxy - This is the preferred approach, as many newly introduced Internet services have unacceptable vulnerabilities.
- Develop a custom proxy - This is a fairly difficult task and should be undertaken only by very sophisticated technical organizations.

- Pass the service through the firewall - Using what are typically called “plugins,” most application gateway firewalls allow services to be passed directly through the firewall with only a minimum of packet filtering. This can limit some of the vulnerability but can result in compromising the security of systems behind the firewall.

2.2.5.1.3 Hybrid or Complex Gateways

Hybrid gateways combine two or more of the above firewall types and implement them in series rather than in parallel. If they are connected in series, then the overall security is enhanced; on the other hand, if they are connected in parallel, then the network security perimeter will be only as secure as the least secure of all methods used. In medium to high risk environments, a hybrid gateway may be the ideal firewall implementation.

2.2.5.2 Firewall Architectures

Firewalls can be configured in a number of different architectures, providing various levels of security at different costs of installation and operation. Organizations should match their risk profile to the type of firewall architecture selected. The following sections describe typical firewall architectures.

2.2.5.2.1 Multi-homed host

A multi-homed host is a host (a firewall in this case) that has more than one network interface, with each interface connected to logically and physically separate network segments. A dual-homed host (host with two interfaces) is the most common instance of a multi-homed host.

A dual-homed firewall is a firewall with two network interfaces cards (NICs) with each interface connected to a different network. For instance, one network interface is typically connected to the external or untrusted network, while the other interface is connected to the internal or trusted network. In this configuration, a key security tenet is not to allow traffic coming in from the untrusted network to be directly routed to the trusted network - the firewall must always act as an intermediary. Routing by the firewall shall be disabled for a dual-homed firewall so that IP packets from one network are not directly routed from one network to the other. Figure 2.2-5 depicts dual-homed gateway firewall architecture.

2.2.5.2.2 Screened Host

A screened host firewall architecture uses a host (called a bastion host) to which all outside hosts connect, rather than allow direct connection to other, less secure internal hosts. To achieve this, a filtering router is configured so that all connections to the internal network from the outside network are directed towards the bastion host. If a packet-filtering gateway is to be deployed, then a bastion host should be set up so that all connections from the outside network go through the bastion host to prevent direct Internet connection between the internal network and the outside world. Figure 2.2-6 depicts the screened host firewall architecture.

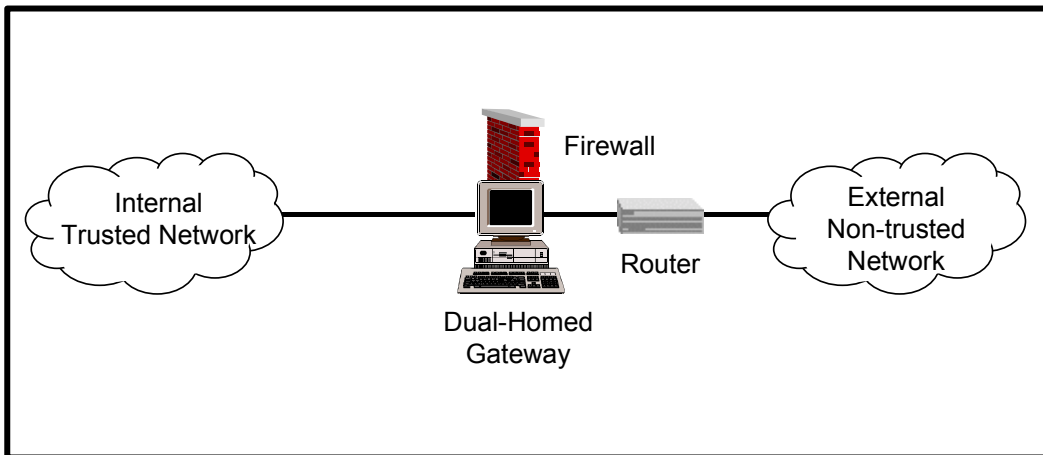


Figure 2.2-5: Dual-Homed Gateway Firewall

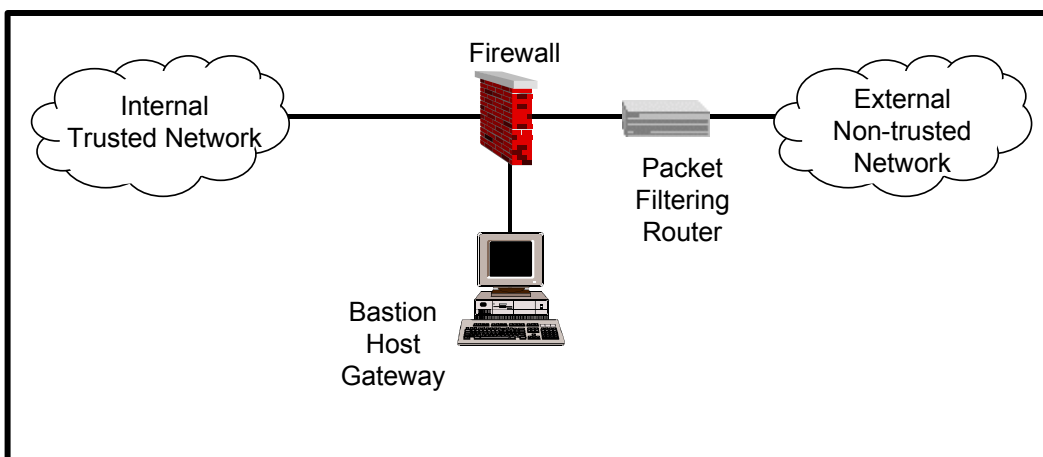


Figure 2.2-6: Screened Host Firewall

2.2.5.2.3 Screened Subnet

The screened subnet architecture is essentially the same as the screened host architecture, but consists of two packet filtering routers and a bastion host, which adds an extra strata of security by creating a network on which the bastion host resides (often called a perimeter network or Demilitarized Zone or DMZ) which is separated from the internal network. This assures that if there is a successful attack on the bastion host, the attacker is restricted to the perimeter network (DMZ) by the screening router that is connected between the internal and perimeter network. Figure 2.2-7 depicts the screened subnet firewall architecture.

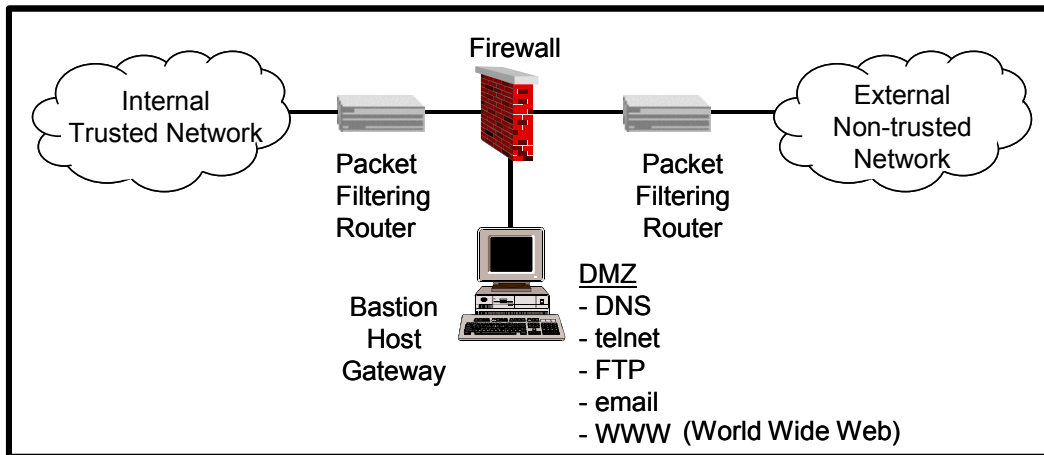


Figure 2.2-7: Screened Subnet Firewall

2.3 TECHNOLOGY, PROTOCOLS, AND STANDARDS FOR VOICE & VIDEO OVER FAST PACKET NETWORKS

2.3.1 Voice and Video Services

The technology discussion for voice and video services has been combined because these signals have similar transport requirements. Both voice and video signals are inherently analog. While they can be (and often are) digitized, the source and sink for this information are invariably analog devices (e.g., ear, mouth or eyes). The nature of voice and video information makes it sensitive to delay, especially delay variations (jitter). Furthermore, unlike data, where requests for retransmits are meaningful and useful (e.g., use of TCP); voice and video applications cannot tolerate the delay associated with retransmissions. Consequently, voice and video are typically streamed, without acknowledgements (ACKS), negative acknowledgements (NACKS), and retransmissions. Hence, when using the IP protocol stack, User Datagram Protocol (UDP), instead of TCP is used with voice and video.

The emphasis of this section will be on the delivery of voice over fast packet networks. While the FAA has videoconferencing requirements, the predominate communications requirement in the NAS, both now and for the foreseeable future, is voice telephony.

2.3.2 Applicable Standards and Protocols

Voice and video can be implemented across ATM, Frame Relay, and IP data networks. However, the ubiquitous presence of IP, especially in the Local Area Network (LAN), makes it an ideal candidate for implementing packet-based telephony. Table 2.3-1 presents a matrix of ATM, Frame Relay, and IP protocol applicability to various important telephony requirements.

An interpretation of Table 2.3-1 is that while voice may be transported over any packet network, the future end-to-end solutions will undoubtedly contain some aspect of IP. There are two major sets of standards that support transmission of voice and video over IP based packet networks: H.323, and

Session Initiation Protocol (SIP). Both of these have strong industry support, and only time will tell which one will dominate the end-user market. A third protocol set, the Media Gateway Control Protocol (MGCP), is not yet fully standardized.

Table 2.3-1: Suitability of ATM, Frame Relay, and IP Protocols to WAN, LAN, and Application Telephony Requirements⁷

Telephony Capability	ATM	Frame Relay	IP	
Voice Coding and Packetization	✓	✓	✓	← WAN
Voice Transport over WAN	✓	✓	✓	
Call management across the network (trunkside)	✓	✓	✓	
Voice Transport over LAN			✓	← LAN
Packet-enabled Voice Terminals			✓	
Call management at lineside			✓	
Integrated Presentation Layer (user interface, etc)			✓	← Applications
Integrated Business and Productivity Applications			✓	
Integrated Management (directory, policy, etc)			✓	

H.323 is an established standards set, developed and published by the International Telecommunications Union-Transmission Systems and Media (ITU-T) organization. The key strength of H.323 is its maturity, which has allowed a number of software vendors to develop robust implementations. The standard's maturity has also allowed the various vendors to eliminate interoperability issues.

SIP is a proposed standard in the IETF standardization process. SIP provides a means to communicate call-control information from end devices or proxy servers to each other or to gateway devices. This protocol is the result of the Multi-party Multimedia Session Control (MMUSIC) working group of the IETF.

MGCP provides a means to interconnect a large number of IP telephony gateways. The specification was developed by various companies and was published as an informative request for comment (RFC 2705) by the IETF. MGCP is a merger of the Simple Gateway Control Protocol and the Internet Protocol Device Control protocols. A revised version of MGCP, under the name of H.248, is being developed by the Megaco working group of the IETF and will be published as an IETF standards track RFC. This group is coordinating the development of the revised version with ITU-T Sub-Group-16.

2.3.2.1 H.323

The H.323 standard provides a foundation for audio, video, and data communications across IP-based networks, including the Internet. ITU's Study Group 16 approved the specification in 1996. Version 2 was approved in January 1998. H.323 has the support of many computing and communications companies and organizations, including Intel, Microsoft, Cisco, and IBM. Figure 2.3-1 shows the scope of the H.323 body of standards. From the figure, it is clear that audio, video and data interfaces are all defined, as well as a set of system control protocols.

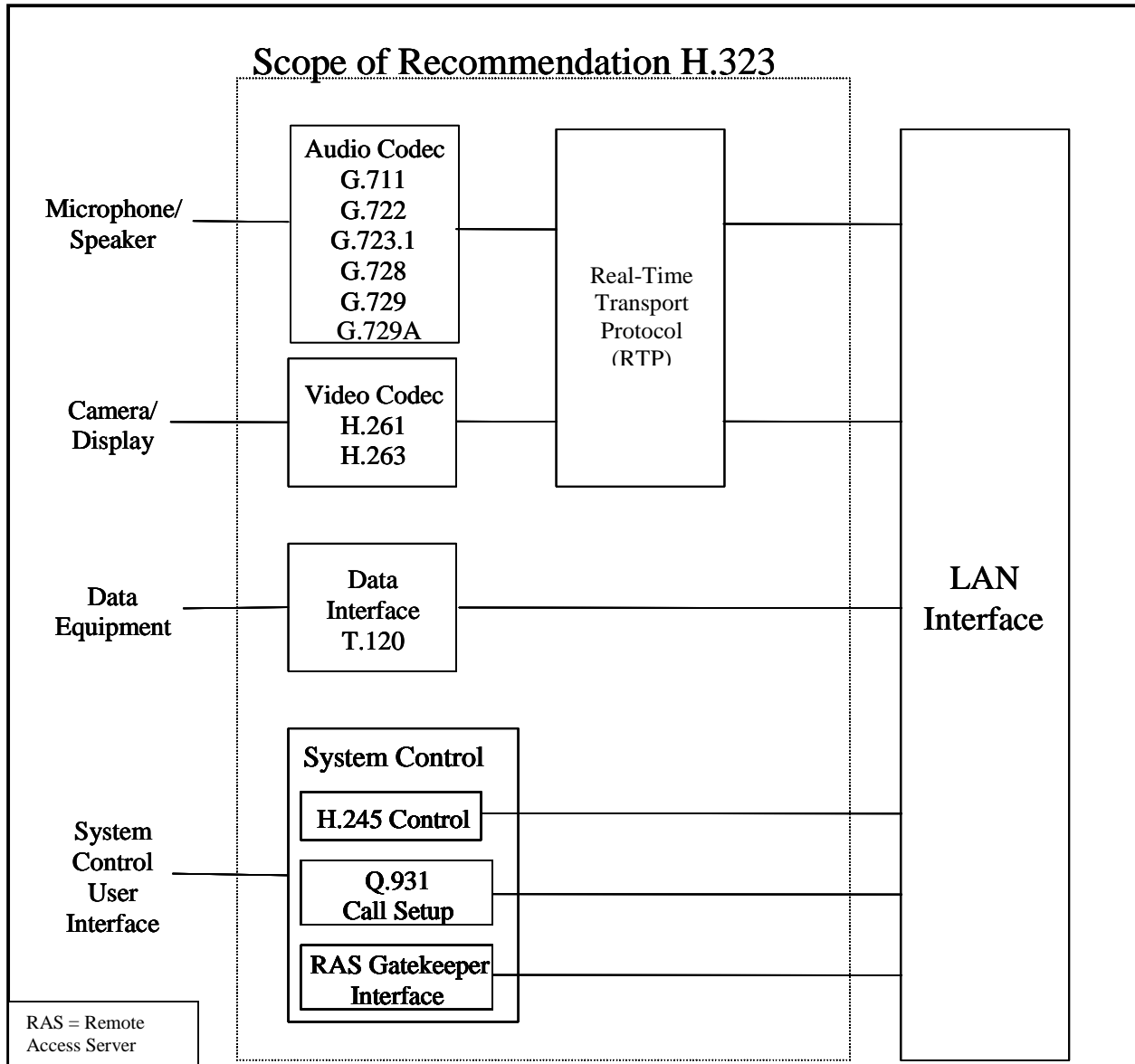


Figure 2.3-1: System Control, Audio, Video, and Data Specifications of H.323

2.3.2.1.1 H.323 Architecture

Figure 2.3-2 provides an overview of the H.323 architecture. This architecture consists of a Multi-point Control Unit (MCU), gatekeeper, H.323 terminals, and gateway(s). The functionality of these devices is described below.

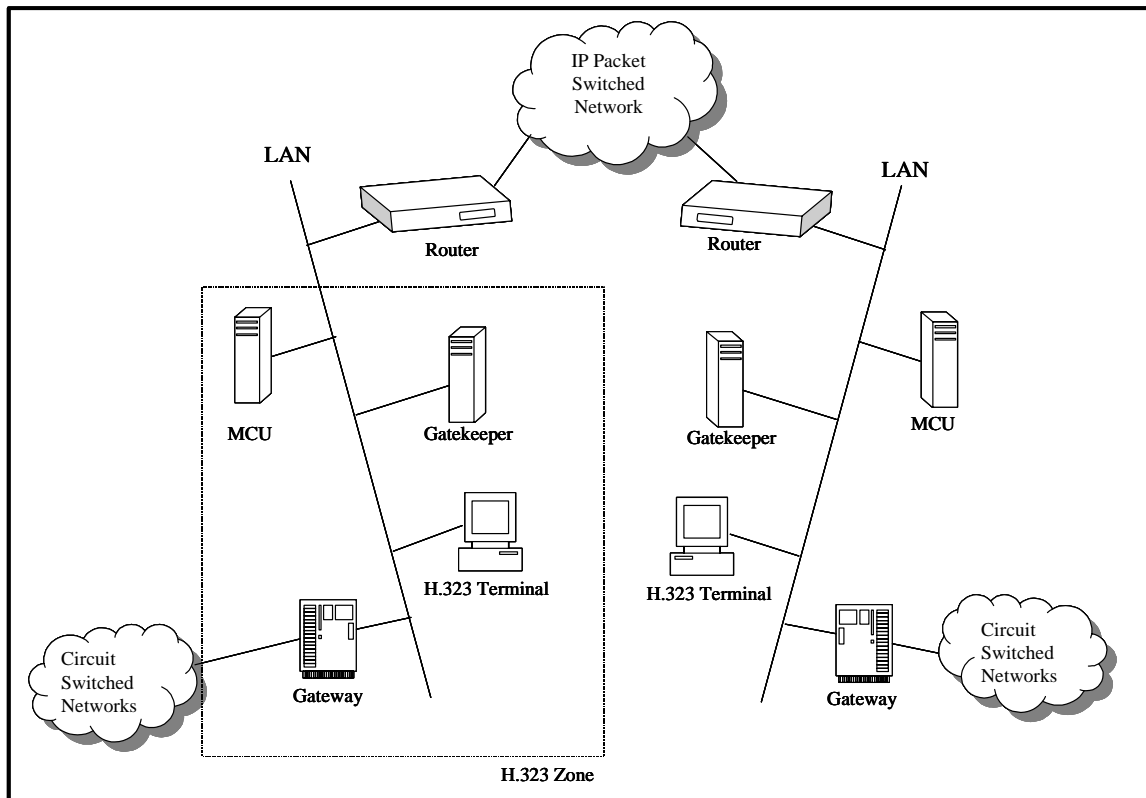


Figure 2.3-2: H.323 Architecture

- **MCU** – Supports conferences between three or more endpoints. It contains a multipoint controller for signaling. It may contain multipoint processors for media stream processing. It can be standalone or integrated into a gateway, gatekeeper, or terminal.
- **Gatekeeper** – Manages a zone (collection of H.323 devices). To conform to the standard, this device must perform the required functions of address translation, admissions control, and bandwidth control. Optionally, gatekeepers may provide for call authorization, bandwidth management, supplementary services, directory services, and call management services.
- **H.323 Terminal** – Endpoint on a LAN. This supports real-time, two-way communications with another H.323 entity. It must support voice (audio codecs) and signaling (Q.931, H.245, RAS). It optionally supports video and data.
- **Gateway** – This device is required to provide interoperability between different networks (e.g., the Public Switched Telephone Network (PSTN) and the H.323 zone). The gateway must convert both the signaling messages and the media (voice) content.

H.323 is part of a larger series of communications standards that enable videoconferencing across a range of networks. Known as H.32x, this series includes H.320 and H.324, which address Integrated Services Digital Network (ISDN) and PSTN communications, respectively. The H.32x body of standards is tabulated in Table 2.3-2. The H.323 architecture in relationship to the H.32x standards universe is shown in Figure 2.3-3.

Table 2.3-2: H32x Standards Universe

	H.320	H.321	H.322	H.323V1/V2	H.324
Approval Date	1990	1995	1995	1996/1998	1996
Network	Narrowband switched digital ISDN	Broadband ISDN ATM LAN	Guaranteed bandwidth packet switched networks	Non-guaranteed bandwidth packet switched networks, (Ethernet)	PSTN or POTS, the analog phone system
Video	H.261 H.263	H.261 H.263	H.261 H.263	H.261 H.263	H.261 H.263
Audio	G.711 G.722 G.728	G.711 G.722 G.728	G.711 G.722 G.728	G.711 G.722 G.728 G.723 G.729	G.723
Multiplexing	H.221	H.221	H.221	H.225.0	H.223
Control	H.230 H.242	H.242	H.242 H.230	H.245	H.245
Multipoint	H.231 H.243	H.231 H.243	H.231 H.243	H.323	
Data	T.120	T.120	T.120	T.120	T.120
Communications Interface	I.400	AAL I.363 AJM I.361 PHY I.400	I.400&TCP/IP	TCP/IP	V.34Modem

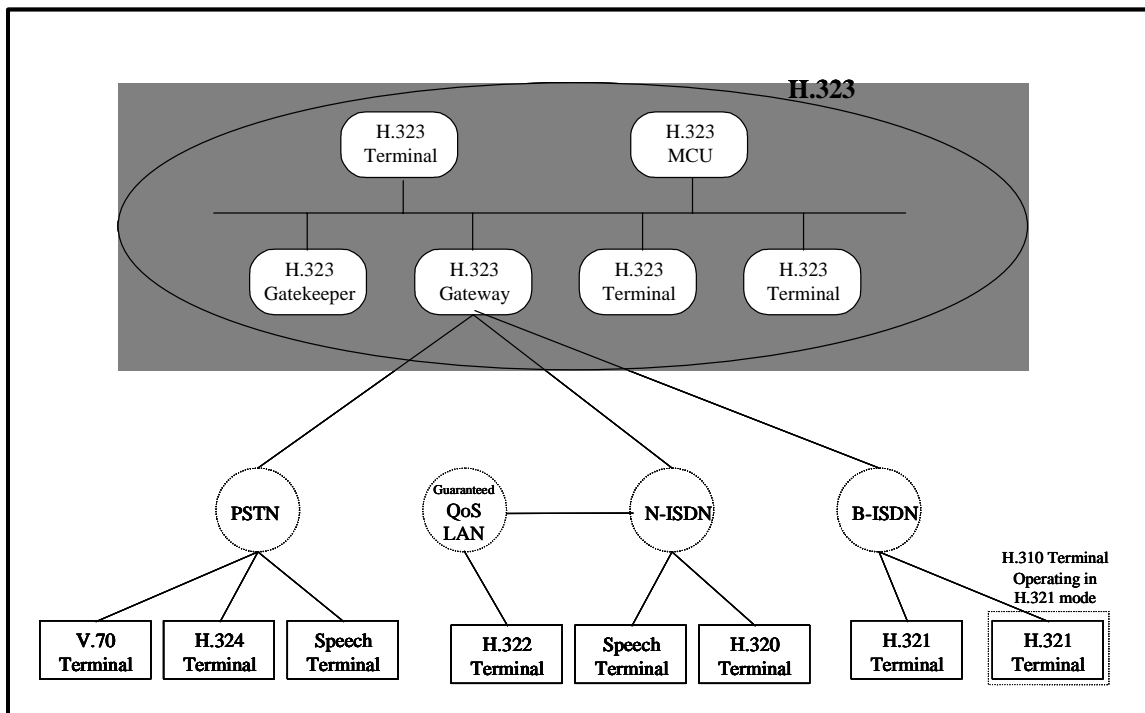


Figure 2.3-3: H.323 Architecture Relationship to the H.32x Standards Universe

2.3.2.2 SIP

SIP is a signaling protocol for Internet Protocol conferencing and telephony. SIP was developed within the IETF MMUSIC working group, with work proceeding in the IETF SIP working group. SIP was proposed as a standard on February 2, 1999, and published as RFC 2543 on March 17, 1999 by the IETF. Manufacturers have been engaged in bake-offs – a colloquial term used to describe interoperability testing of standards implementations – since April 1999. Table 2.3-3 shows the location, dates, and number of participating organizations of SIP bake-offs that have been held to date.

Table 2.3-3: SIP Bake-offs

Bakeoff Number	Host	Date	Number of Organizations	Number of Attendees
1	Columbia University, New York, NY	April 8-9, 1999	16	36
2	Pulver.com, Melville, NY	August 5-6, 1999	15	39
3	Ericsson	December 6-8, 1999	31 teams (26 companies)	
4	3Com, Schaumburg (Chicago), Illinois	April 17-19, 2000	46 teams (36 companies)	108
5	Pulver.com, Melville, New York	August 8-10, 2000	50 teams (44 companies)	143
6	Sylantro, Campbell, CA	December 5-7, 2000	—	—
7	ETSI, France (tentative)	April 2001	—	—
8	Ubiquity	August 2001	—	—

These kinds of interoperability tests are a key component of the IETF standards process. Requests for Comments (RFC - IETF official standards) progress through three phases of maturity as the protocols are rolled out and deployed. SIP is currently at the first phase: proposed standard RFC, and interoperability of every feature must be demonstrated in order to advance to the next stage: draft standard RFC.

2.3.2.2.1 SIP Architecture

The SIP architecture consists of User Agent Clients (UAC), User Agent Servers (UAS), SIP terminals, Proxies, Redirect Servers, and Location Servers. The function of each component is described below.

- **UACs** – Caller application that initiates and sends SIP requests.
- **UASs** – Receives and responds to SIP requests on behalf of clients; accepts, redirects, or refuses calls.
- **SIP terminals** – Supports real-time, two-way communication with another SIP entity. It supports both signaling and media (similar to H.323 terminal), and contains UAC.
- **Proxies** – Contacts one or more clients or next-hop servers and passes the call requests further. It contains UAC and UAS.
- **Redirect Servers** – Accepts SIP requests, maps the address into zero or more new addresses and returns those addresses to the client. It does not initiate SIP requests or accept calls.

- **Location Servers** – Provides information about a caller's possible locations to redirect and proxy servers. It may be co-located with a SIP server.

Figure 2.3-4 provides a graphical overview of the SIP architecture.

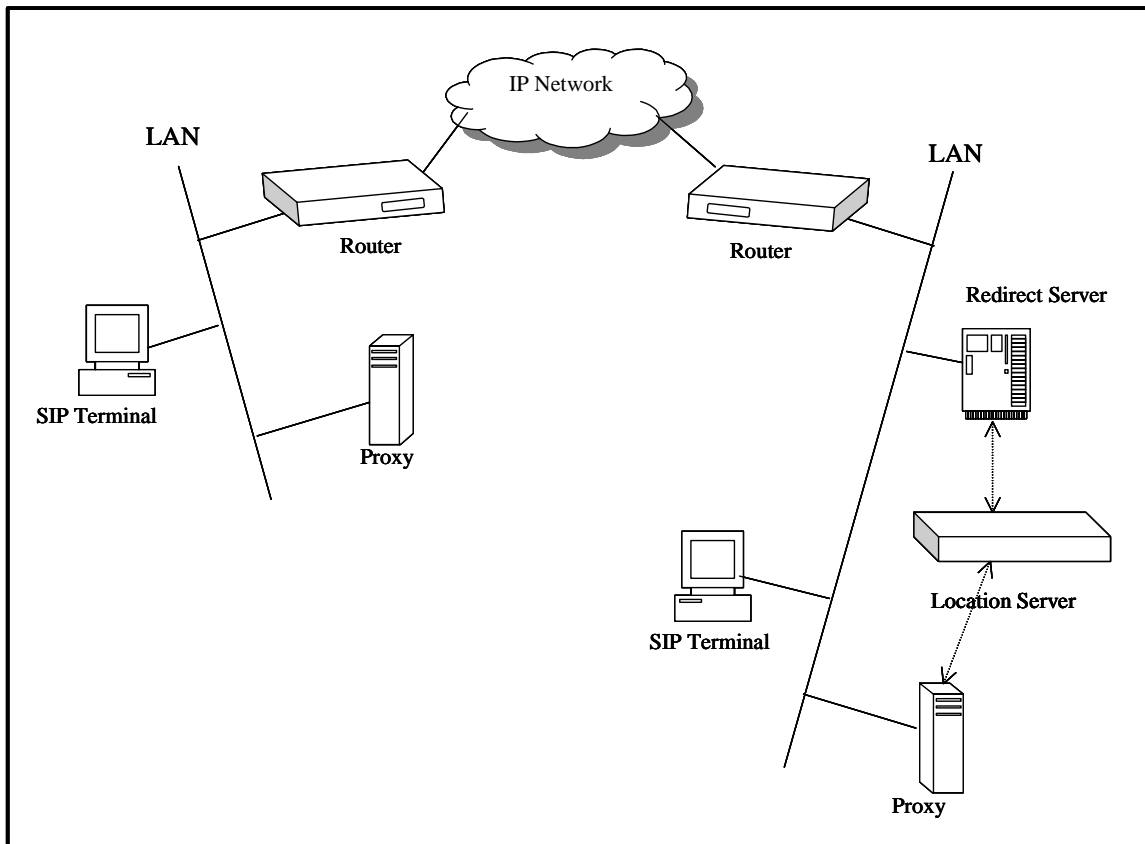


Figure 2.3-4: SIP Architecture

2.3.2.3 MGCP

MGCP is a simple control protocol that enables a network entity (responsible for setting up calls) to control the media streaming devices that perform the actual IP voice streaming. MGCP is the result of a merger between the simple gateway control protocol (SGCP) from Bellcore, and the IP device control (IPDC) from Level 3 Communications. The description of this protocol (Version 1.0) is documented in RFC 2705.

MGCP allows software programs known as call agents or media gateway controllers to externally control and manage media streaming devices, or media gateways, at the edge of multiservice packet networks. This separation between audio-streaming functions and call-control functions enhances system operation and simplifies operation of the media gateway.

Media gateways can be VoIP gateways, voice over ATM gateways, modem banks, cable modems, set-top boxes, and soft Private Branch Exchanges (PBXs).

2.3.2.3.1 MGCP Architecture

MGCP assumes a software-based call-control architecture, where the call-control intelligence is outside the media gateways and handled by external call-control elements. MGCP assumes that these call-control elements, or call agents, will synchronize with each other to send coherent commands to the gateways under their control. MGCP does not define a mechanism for synchronizing call agents. Essentially, MGCP is a master/slave protocol, where the gateways are expected to execute commands sent by the call agents. As a consequence, the expected behavior of the gateways can be specified. Only those parts of a call-agent implementation that are mandated for proper operation of the protocol (such as timer management) need to be specified.

MGCP assumes a connection model where the basic constructs are endpoints and connections. Endpoints are sources or sinks of data and can be physical or virtual.

MGCP is designed as an internal protocol within a distributed system, appearing externally as a single VoIP gateway. The system consists of a software-implemented call agent or media gateway controller and a media gateway, where the call agent may or may not be distributed over several computer platforms.

The media gateway is a simple, “dumb” end point (brawn), which is capable of performing the media streaming to another media gateway if the session is set up by a call agent on both ends. The media gateways perform the conversion of media signals between circuit-switched and packet networks. The call agent can also connect to a separate signaling gateway when connecting to a Signaling System 7 (SS7)-controlled network.

The call agent is responsible for all network operation, including call initiation. The intelligent call agent uses MGCP to control the endpoints (media gateways). In a simple scenario, where two media gateways under the same call agent need to participate in a call, the call agent will collect events and routing information from the originating media gateways, and route the call to the terminating gateway, using MGCP in both cases. Once the call is established, the voice is transmitted directly between the two gateways by using the real-time transport protocol (RTP).

In a typical configuration, this distributed gateway system can interface on one side with one or more telephony (circuit) switches, and on the other side with H.323-compliant systems.

2.3.2.4 Comparative Analysis of VoIP Protocols

These protocols can be compared in terms of their complexity, extensibility, scalability, and services provided. As an example, H.323 is more complex than SIP. H.323 has hundreds of defined elements

compared to the 37 defined SIP headers. H.323 signaling messages use a binary format, whereas SIP messages are in plain text.

Furthermore, SIP has several mechanisms designed to promote extensibility as new applications are developed. Unknown headers are ignored by default. The Requires header can be used to establish a minimum set of required features. Error codes are hierarchically organized, and header fields are self-describing. SIP provides third-party call control mechanisms, rather than trying to write specifications for the hundreds of telephony services that are currently defined. While H.323 has extensibility mechanisms, they are limited to predefined placeholders for non-standard parameters. Furthermore, H.323 requires full backwards compatibility, causing coding implementations to increase with time.

SIP is also more scaleable than H.323. As an example, H.323 gatekeepers must track the state of a call through its duration, while SIP can operate in a stateless fashion. Hence SIP is more easily scaled to provide large backbone telephony services handling many calls.

SIP would appear to have many advantages over H.323; however, H.323 does have a major advantage as a developed standard (recall that SIP is a draft RFC). Hence H.323 currently has a large share of the market. History has shown that market pressures do not always pick the best technological implementation. In fact, the three standards sets can be viewed as somewhat complementary. In this view, each of these protocols addresses different aspects of the technology needed to develop IP telephony systems. Numerous systems being developed today include one or more of these protocols, often working together⁸.

As noted above, the key strength of H.323 is its maturity, which has allowed a number of software vendors to develop robust implementations. The standard's maturity has also allowed the various vendors to eliminate interoperability issues, permitting the deployment of a wide range of H.323-capable devices into the market.

However, the cost of implementation of H.323 has been an issue when an inexpensive end device is required. The complexity of the standard requires significant processing capability at the end device. H.323 works well in environments where there is enough processing capability to implement the call control and media processing. Accordingly, H.323 has gained its strongest support as an IP telephony solution for enterprises.

MGCP is particularly suited to large deployed applications because it was defined to solve a specific problem with large deployed systems. Use of MGCP allows for good integration into the SS7 network, which gives greater control and throughput in handling calls. MGCP splits the media handling and signaling functions, thus providing a simpler implementation that can be developed by multiple vendors.

MGCP is too complex for smaller applications. Clearly the home for MGCP is in the carrier space — delivering thousands of lines of IP telephony.

The expandable nature of the SIP protocol allows future capabilities to be easily defined and quickly implemented. It is simple and easy to embed into inexpensive end-user devices. The protocol was designed to ensure interoperability and enable different devices to communicate. Non-telephony developers find the protocol easy to understand.

However, SIP is very new, so most applications are in the prototype stage. The protocol has a narrow scope and thus has limited applications by itself; however, it gains flexibility when used with other protocols. SIP is only a small piece of a complete solution. Numerous other software components are required to build a complete IP telephony product.

Low-cost end devices are natural applications for SIP. Devices such as wireless phones, set-top cable boxes, Ethernet phones, and other devices with limited computing and memory resources are suited to this protocol.

2.3.3 Technology and Market Trends

When assessing any technology, it is important to look at market trends. Cahners In-Stat Group (a market research firm) reported that sales of remote access concentrator and router-based VoIP gateways reached \$741 million in 1999. Cisco, Lucent and 3Com lead in this segment, with year-end market shares of 51 percent, 28 percent and 11 percent, respectively.⁹

From their LAN telephony research, In-Stat believes that the features, applications, and ultimately the pricing of LAN Telephony will ultimately result in the demise of PBX systems. IP packets will rise over Ethernet technology due to its openness and ubiquity. Benefits will include complete handset and extension portability to remote locations, integration with contact management software and worldwide IP based contact centers. Following interoperability between vendors, eventual retail of packet handsets to consumers will occur causing the industry to ignite.

International Data Corporation echoes these predictions. They project revenue from IP-telephony services to reach \$480 million in 1999, with a compounded annual growth rate of 108%. Predicted industry revenues by 2003 are \$19 billion¹⁰.

2.4 TECHNOLOGY, PROTOCOLS AND STANDARDS FOR ENTERPRISE MANAGEMENT

2.4.1 Introduction

Enterprise Management refers to an architecture that provides management solutions to make it easier for an organization to centrally manage all of its computing resources, from hardware to networks to servers to applications and even desktop workstations.¹¹ It includes Network Monitoring and Management, which specifically relates to the management of the network infrastructure, including networking devices,

links, network performance, etc, as well as application data management and support of other information system elements including the following:

- Management of IP address space
- Time distribution services
- Network directory services

The following sections provide a discussion of each of these four aspects of Enterprise Management, and particularly the services and technology available to provide them.

2.4.2 Network Monitoring and Management

Network service providers map customer performance requirements to services using SLAs. SLAs provide an understanding between the service providers and their customers, and provide for service providers to report on service performance using a customer-oriented tracking system. To provide proof of performance, and to effectively manage their networks, service providers monitor both historical and near real-time network performance data. Near real-time performance data allows service providers to react to critical network situations as they occur, while historical network performance data analysis detects trends that help precisely locate network trouble spots. By revealing trends, service providers can take action to modify network capacity. Complementary historical data analysis helps service providers decide where to add, shift, or remove network traffic.

A monitoring system is a cohesive, integrated set of elements for collecting information, offering the appropriate analysis and responding as needed. Remote monitoring (RMON) agents and analysis tools are key elements of the monitoring system. RMON agents gather information for the analysis tools. They are embedded in network products, such as hubs and switches, and are available as stand-alone probes and in network interface cards. RMON agents gather physical and data link layer data for a single LAN segment. RMON2 agents collect data at the network and application layers for analysis of flows between parts of the enterprise network. Combining these agents gives detailed information about any LAN segment as well as end-to-end traffic analysis across complex networks.

In addition to RMON agents, analysis tools are required. Analysis tools transform the collected data into useful information, offering deeper insight for network and system administrators. There is a set of key attributes to consider:

- **Granularity** - Tools must extract and present specific pieces of information from the incoming flood of data.
- **Customization** - Tools need to present information in useful ways for individual administrators.
- **Ease-of-use** - Tools should be simple to install and use, with graphical interfaces.

Finally, analysis tools must provide actionable information, guiding an administrator or management tool to the appropriate response.

Identifying a (potential) problem is not sufficient. Administrators need enough information to know what to do next or they may need sophisticated tools that offer suggestions. Automated responses save staff time, reduce errors, and restore services quickly. Figure 2.4-1 shows the use of RMON agents to collect network performance information. This information is then sent to network management workstations, where the analysis tools reside.

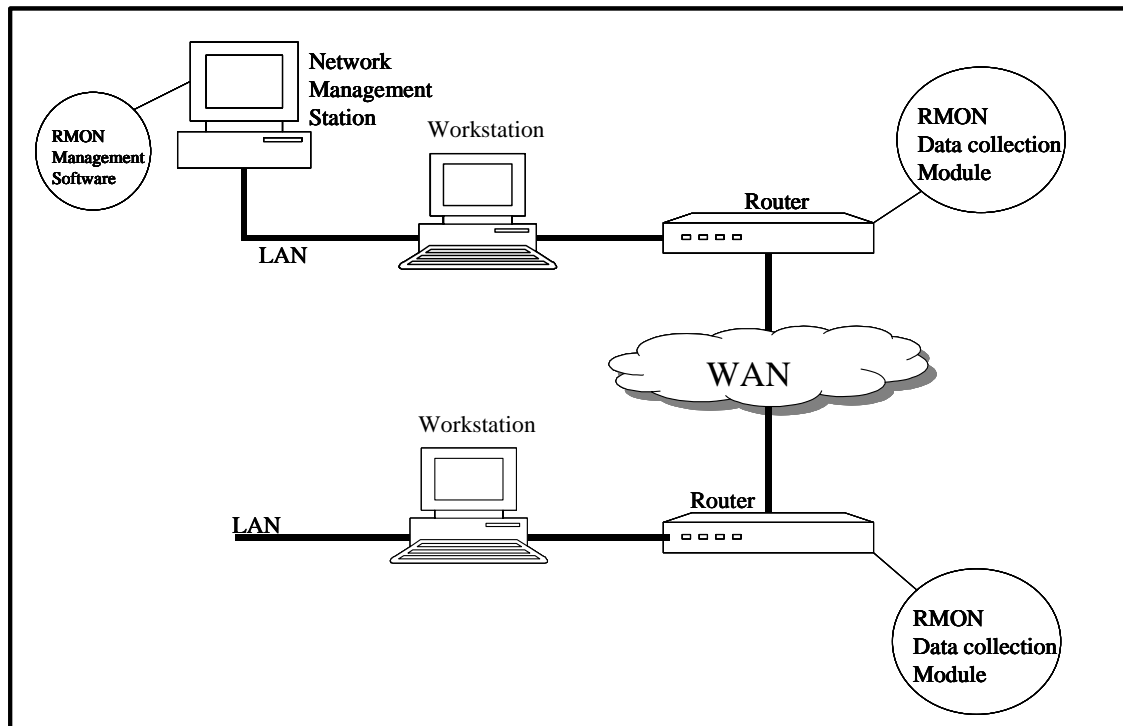


Figure 2.4-1: Network Monitoring and Management Configuration

2.4.3 Management of IP Address Space

IPv4 addresses are 32 bit values: “byte.byte.byte.byte” where each byte of data is a number from 0 to 255. The address space is hierarchical with the leftmost byte at the top of the hierarchy. There are three classes of IP address licenses:

- Class A license: N.x.x.x allows 2^{24} addresses (>16 million).
- Class B license: N.M.x.x allows 2^{16} addresses (>65,000).
- Class C license: N.M.O.x allows 2^8 addresses (256).
- Other Classes: In addition to the three most popular classes, there are two additional classes. Class D addresses have the leading four bits set to 1-1-1-0 and are used to support IP multicasting. Class E addresses have the leading four bits set to 1-1-1-1 and are reserved for experimental use.

There are both public and private addresses. Public addresses are licensed by central authority and are unique worldwide. Private addresses for closed networks are defined by RFC 1597. The defined private address space is shown in Table 2.4-1.

Table 2.4-1: Defined IP Private Address Space

Class	Number	Address Space
A	1	10.0.0.0 – 10.255.255.255
B	16	172.16.0.0 – 172.31.255.255
C	256	192.168.0.0 – 192.168.255.255

Domain names are the familiar and easy-to-remember names for Internet computers (e.g., "www.ecommerce.gov"). They map to unique IP numbers (e.g., 98.37.241.30) that serve as routing addresses on the Internet. The DNS translates Internet names into the IP numbers needed for transmission of information across the network.

The activities required to manage an IP Address Space include:

- Allocation of IP addresses to facilities/programs.
- Assignment of IP addresses to hosts.
- Adoption of a naming convention that maps names (based on a hierarchical naming structure) to IP addresses.
- Implementation of the DNS: location and number of Domain Name Servers.

2.4.3.1 Allocation of IP Addresses to Facilities/Programs and Hosts

Every Internet computer has a unique IP number. This system is coordinated by allocating blocks of numerical addresses to regional IP registries American Registry for Port Numbers (ARIN) in North America, Réseaux IP Européens (RIPE) in Europe, and Asia Pacific Network Information Center (APNIC) in the Asia/Pacific region), under contract with Defense Advanced Research Projects Agency (DARPA). In turn, larger Internet service providers apply to the regional IP registries for blocks of IP addresses. The recipients of those address blocks then reassign addresses to smaller Internet service providers and to end-users.

2.4.3.2 Management of the System of Registering Names for Internet Users

The domain name space is constructed as a hierarchy. It is divided into top-level domains (TLDs), with each TLD subdivided into second-level domains (SLDs), and so on. More than 200 national, or country-code TLDs (ccTLDs) are administered by their corresponding governments or by private entities with the appropriate national government's acquiescence. Small sets of TLDs do not carry any national identifier, but denote the intended function of that portion of the domain space. For example, ".com" was

established for commercial users, “.org” for not-for-profit organizations, and “.net” for network service providers.

2.4.3.3 Operation of the Root DNS Server System

The root server system is a set of thirteen file servers, which together contain authoritative databases listing all TLDs. Currently, NSI operates the "A" root server, which maintains the authoritative root database and replicates changes to the other root servers on a daily basis. Different organizations, including NSI, operate the other 12 root servers. The U.S. Government plays a role in the operation of about half of the Internet's root servers. Universal name consistency on the Internet cannot be guaranteed without a set of authoritative and consistent roots. Without such consistency messages could not be routed with any certainty to the intended addresses.

In July 1997, the President directed the Department of Commerce (DoC) to privatize DNS management to increase competition and facilitate international participation. Following a period of public comment, the DoC, through its National Telecommunications and Information Administration (NTIA), issued a statement of policy entitled Management of Internet Names and Addresses (known as the "White Paper") which called for the formation of a new nonprofit corporation. In September 1998, the Internet Corporation for Assigned Names and Numbers (ICANN) was formed to take over IANA's responsibilities and to operate without government funding.

2.4.3.4 IPv6/IPv4 Address Resolution

Legacy IP networks use the IPv4 protocol. As the next generation IP protocol (IPv6) is phased in, transition mechanisms are required to allow legacy equipment to resolve the new IPv6 addresses. RFC 1933 specifies IPv6 Transition Mechanisms. The two methods that are specified are the Dual IP layer, and IPv6-Over-IPv4 Tunneling.

2.4.3.4.1 Dual IP Layer

The most straightforward way for IPv6 nodes to remain compatible with IPv4-only nodes is by providing a complete IPv4 implementation. IPv6 nodes that provide a complete IPv4 implementation in addition to their IPv6 implementation are called "IPv6/IPv4 nodes." IPv6/IPv4 nodes have the ability to send and receive both IPv4 and IPv6 packets. They can directly interoperate with IPv4 nodes using IPv4 packets, and also directly interoperate with IPv6 nodes using IPv6 packets.

2.4.3.4.2 IPv6 over IPv4 Tunneling

Encapsulating IPv6 packets within IPv4 headers to carry them over IPv4 routing infrastructures is called tunneling. Two types of tunneling are employed: configured and automatic. Configured tunneling is IPv6-over-IPv4 tunneling, where the IPv4 tunnel endpoint address is determined by configuration information on the encapsulating node. Automatic tunneling is IPv6-over-IPv4 tunneling, where the IPv4

tunnel endpoint address is determined from the IPv4 address embedded in the IPv4-compatible destination address of the IPv6 packet¹².

RFC 1933 defines four deployment scenarios requiring IPv6 tunneling across an IPv4 infrastructure. The four scenarios are shown in Figure 2.4-1.

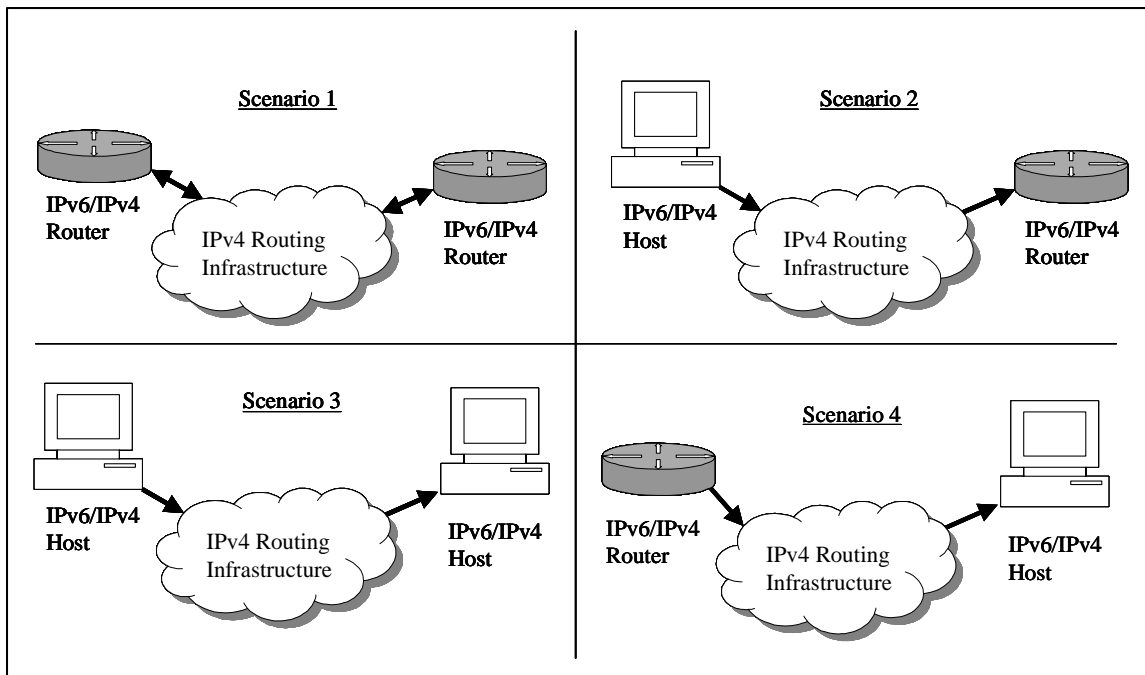


Figure 2.4-1: Tunneling Scenarios

The two tunneling techniques -- automatic and configured -- differ primarily in how they determine the tunnel endpoint address. Most of the underlying mechanisms are the same.

The entry node of the tunnel (the encapsulating node) creates an encapsulating IPv4 header and transmits the encapsulated packet. The exit node of the tunnel (the decapsulating node) receives the encapsulated packet, removes the IPv4 header, updates the IPv6 header, and processes the received IPv6 packet. Figure 2.4-2 shows this process at the highest level of abstraction.

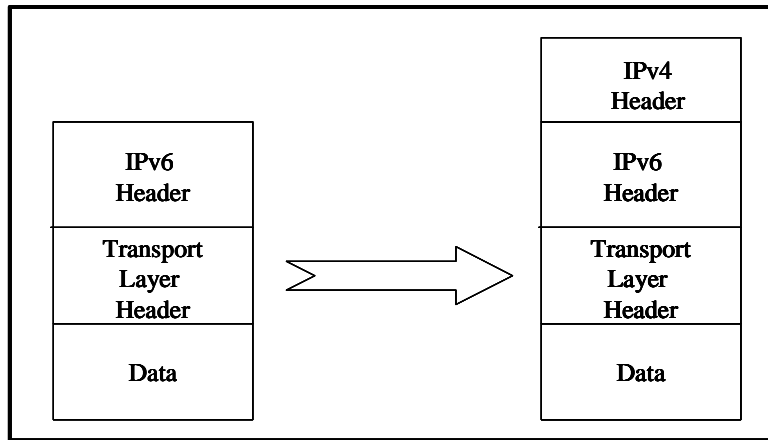


Figure 2.4-2: Encapsulation Process

When encapsulating an IPv6 packet in an IPv4 datagram, the IPv4 header fields are set as shown in Table 2.4-2.

Table 2.4-2: Values to Use in IPv4 Header When Encapsulating IPv6 Packet

IPv4 Header Field	Value to Use
Version	4
IP Header Length in 32-bit words	5 (There are no IPv4 options in the encapsulating header).
Type of Service	0
Total Length	Payload length from IPv6 header plus length of IPv6 and IPv4 headers (i.e., a constant 60 bytes).
Identification	Generated uniquely as for any IPv4 packet transmitted by the system
Flags	Set the Don't Fragment (DF) flag. Set the More Fragments (MF) bit as necessary if fragmenting.
Fragment offset	Set as necessary if fragmenting.
Time to Live	Set in implementation-specific manner.
Protocol	41 (Assigned payload type number for IPv6)
Header Checksum	Calculate the checksum of the IPv4 header.
Source Address	IPv4 address of outgoing interface of the encapsulating node.
Destination Address	IPv4 address of tunnel endpoint.
Any IPv6 options are preserved in the packet (after the IPv6 header)	

The DNS is used in both IPv4 and IPv6 to map hostnames into addresses. A new resource record type named "AAAA" has been defined for IPv6 addresses. Since IPv6/IPv4 nodes must be able to interoperate directly with both IPv4 and IPv6 nodes, they must provide resolver libraries capable of dealing with IPv4 "A" records as well as IPv6 "AAAA" records.

When an IPv4-compatible IPv6 addresses is assigned to an IPv6/IPv4 host that supports automatic tunneling, both A and AAAA records are listed in the DNS. The AAAA record holds the full IPv4-compatible IPv6 address, while the A record holds the low-order 32-bits of that address. The AAAA

record is needed so that queries by IPv6 hosts can be satisfied. The A record is needed so that queries by IPv4-only hosts, whose resolver libraries only support the A record type, will locate the host.

DNS resolver libraries on IPv6/IPv4 nodes must be capable of handling both AAAA and A records. However, when a query locates an AAAA record holding an IPv4-compatible IPv6 address, and an A record holding the corresponding IPv4 address, the resolver library need not necessarily return both addresses. It has three options:

- Return only the IPv6 address to the application.
- Return only the IPv4 address to the application.
- Return both addresses to the application.

The selection of which address type to return in this case, or, if both addresses are returned, in which order they are listed, can affect what type of IP traffic is generated. If the IPv6 address is returned, the node will communicate with that destination using IPv6 packets (in most cases encapsulated in IPv4); if the IPv4 address is returned, the communication will use IPv4 packets.

The way that DNS resolver implementations handle redundant records for IPv4-compatible addresses may depend on whether that implementation supports automatic tunneling, or whether it is enabled. For example, an implementation that does not support automatic tunneling would not return IPv4-compatible IPv6 addresses to applications because those destinations are generally only reachable via tunneling. On the other hand, those implementations in which automatic tunneling is supported and enabled may elect to return only the IPv4-compatible IPv6 address and not the IPv4 address.

2.4.4 Time Distribution Services

Accurate and stable time synchronization is vital to all modern digital networks. As NAS communications evolve toward an integrated, distributed nationwide digital network, time distribution becomes an important part of an integrated network management system. This section presents basic synchronization concepts and a discussion of the Network Time Protocol.

2.4.4.1 Synchronization Basics

Over the last forty years, commercial digital telecommunications networks have evolved sophisticated, hierarchical synchronization architectures. Most of these modern digital telecommunications networks, as well as most national navigation systems, rely on the distribution of accurate timing through the use of Primary Reference Sources (PRs) and derivative timing sources that have their timing traceable to a national Master Clock (MC) maintained by the United States Naval Observatory (USNO). This MC is derived from an ensemble of 50 high-quality cesium and 14 cavity-tuned hydrogen maser frequency standards¹³, the largest reference time source ensemble in the world and the largest contributor to Coordinated Universal Time (UTC).

As part of the hierarchical synchronization system, timing sources are assigned a “stratum” level based on three parameters:

- **Free-run accuracy** - A measure of the time accuracy of the timing source not steered (controlled) by an external timing reference.
- **Holdover stability** – How well a timing source can independently maintain its specified accuracy over time.
- **Pull In/Hold In** – A timing source’s ability to achieve/maintain synchronization with a reference that may be off-frequency.

These stratum levels are defined in Table 2.4-3. A PRS is defined as equipment that provides a timing signal whose long-term fractional frequency stability is maintained at 1×10^{-11} or better with verification to UTC. It should be noted that, while all Stratum 1 sources may be PRCs, not all PRCs are necessarily Stratum 1.

Table 2.4-3: Stratum Levels

Stratum Levels	Accuracy	Minimum Stability
Stratum 1	1×10^{-11}	N/A
Stratum 2	1.6×10^{-8} (.0025 Hz at 1.544 MHz)	1×10^{-10} /day
Stratum 3	4.6×10^{-6} (7 Hz at 1.544 MHz)	< 255 slips on any connecting link during the initial 24 hours
Stratum 4	32×10^{-6} (50 Hz at 1.544 MHz)	N/A

There are numerous methods to implement timing distribution for a network, depending on the network’s timing requirements, sensitivity to cost, and the accessibility to the various sources of accurate timing. Standalone cesium-based stratum 1 clocks and rubidium-based stratum 2 clocks can be obtained and augmented by GPS based systems to serve as PRCs. Other types of equipment can be used to obtain timing through network service providers, including wireless carriers.

For IP networks, the Network Time Protocol (NTP) is used to synchronize the clocks of hosts and routers to national standard time. NTP will be discussed in more detail in the following sections.

2.4.4.2 Network Synchronization – NTP¹⁴

2.4.4.2.1 NTP Introduction and Overview

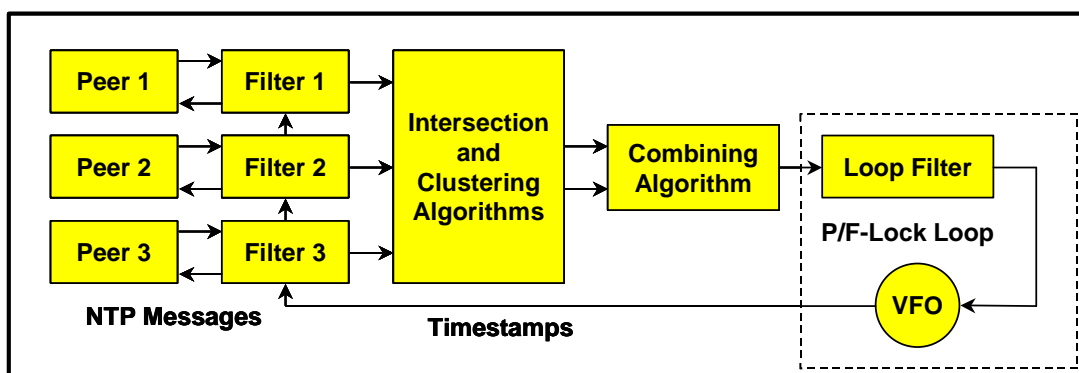
NTP has become the standard method for synchronizing IP based networks. There are well over 100,000 NTP peers deployed in the Internet and its tributaries all over the world. NTP provides nominal accuracies of low tens of milliseconds on WANs, submilliseconds on LANs, and submicroseconds using

a precision time source such as a cesium oscillator or Global Positioning Satellite (GPS) receiver. Originally developed in UNIX, the UNIX NTP daemon has been ported to almost every workstation and server platform available today - from PCs to Crays - Unix, Windows, VMS and embedded systems. As with other Internet standards, NTP has been developed through the IETF standards process. The NTP architecture, protocol, and algorithms have been evolved over the last twenty years to the latest NTP Version 4.

For NTP, primary (stratum 1) servers synchronize to national time standards via radio, satellite and modem. Secondary (stratum 2, 3, and 4) servers and clients synchronize to primary servers via a hierarchical subnet. Clients and servers operate in master/slave, symmetric or multicast modes with or without cryptographic authentication. Reliability in NTP is assured by redundant servers and diverse network paths. The designers of NTP have engineered algorithms that reduce jitter, mitigate potential problems with using multiple sources, and avoid improperly operating servers. The NTP system clock is disciplined in time and frequency using an adaptive algorithm responsive to network time jitter and clock oscillator frequency wander.

2.4.4.2.2 NTP Architecture Description

Figure 2.4-3 illustrates a high level view of the NTP architecture. As shown in the figure, multiple servers/peers are used to provide redundancy and diversity. The servers/peers transmit and receive timing message samples using the NTP protocol header and timestamp formats shown in Figure 2.4-4. For each input, clock filters select the best samples from a window of eight time offset samples. The intersection and clustering algorithms pick the best subset of servers believed to be accurate and fault-free. The combining algorithm then computes the weighted average of time offsets from the selected set of servers to provide the best accuracy. Finally, a phase/frequency-lock feedback loop disciplines local clock time and frequency to maximize accuracy and stability.



Note: VFO = Voltage Control Oscillator; P/F = Phase/Frequency

Figure 2.4-3: NTP Architecture

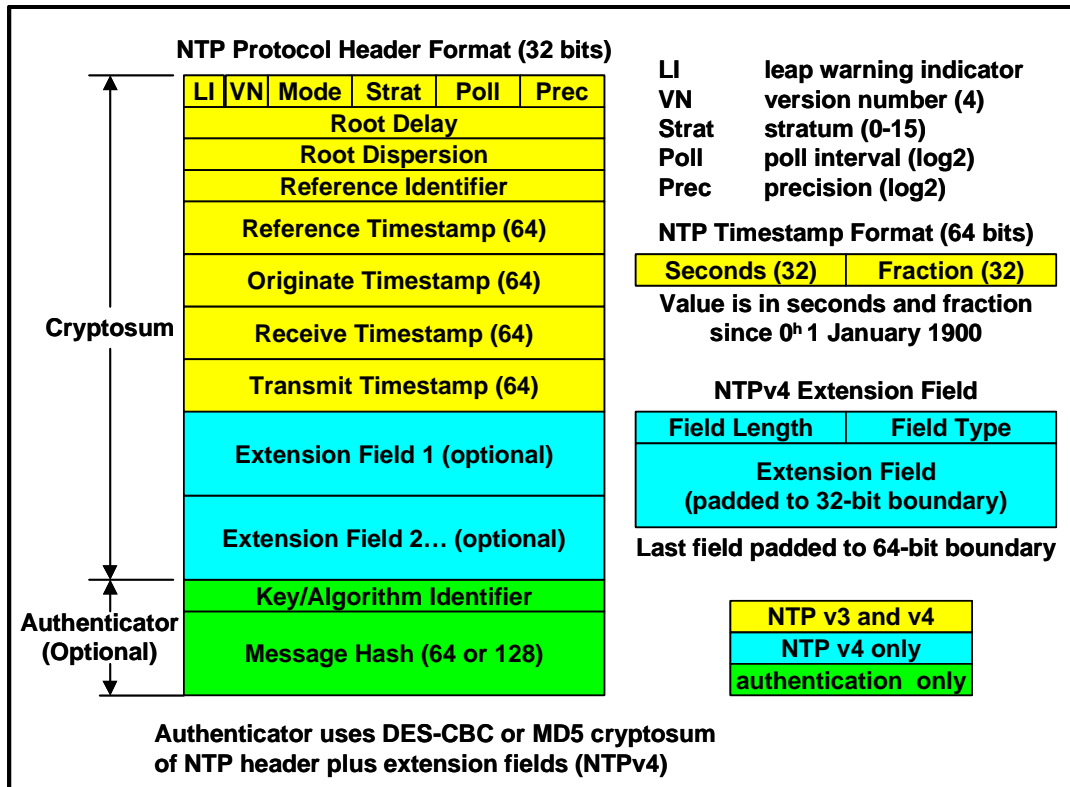


Figure 2.4-4: NTP Protocol Header and Timestamp Formats

2.4.4.2.3 NTP Configuration

NTP can provide network synchronization with a number of different configurations and operating modes, as shown in Figure 2.4-5 (S1 in the figure denotes stratum 1, S2 = stratum 2, etc.). Figure 2.4-5a depicts a workstation configuration, where workstations use the multicast mode with multiple department servers. In Figure 2.4-5b, department servers use client/server modes with multiple campus servers and symmetric modes with each other. Finally, at a higher level, campus servers use client/server modes with up to six different external primary servers, and symmetric modes with each other and external secondary (buddy) servers, as shown in Figure 2.4-5c.

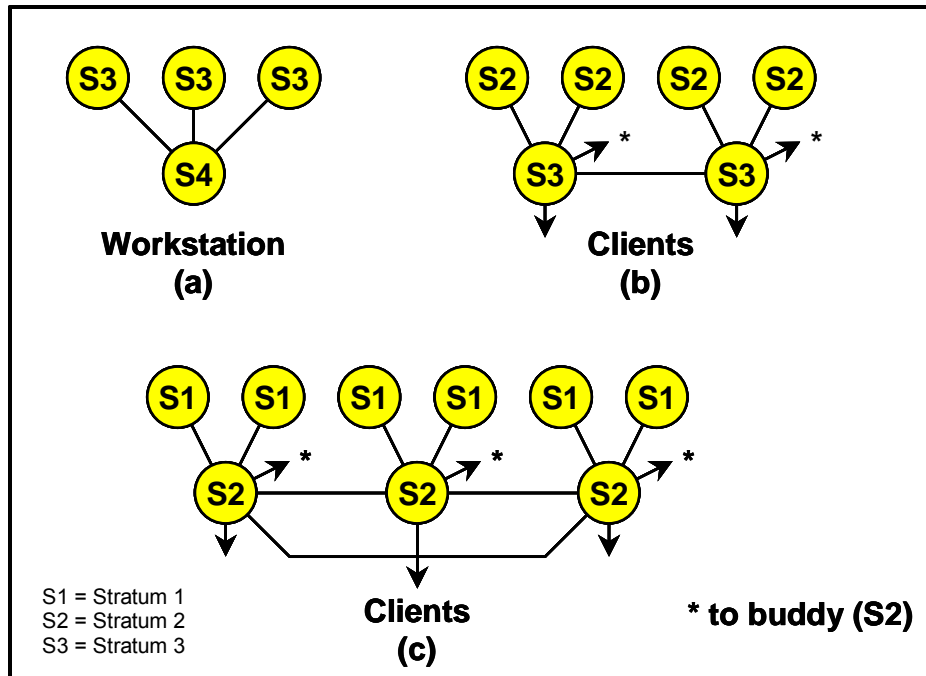


Figure 2.4-5: NTP Configuration

2.4.5 Network Directory Services

Another important aspect of enterprise management is the network directory service. This section provides a brief discussion of network directory services: including their definitions and characterization; the need for directory services, and current directory service standards.

2.4.5.1 Definitions

A network or enterprise directory service in a distributed system provides a means for locating and identifying enterprise users and all available resources in that system. It also provides the means for updating and managing directory components belonging to the enterprise without disruption to other services.

A directory in the context of a network is a listing of information about objects within the network (e.g., object addresses) arranged in some order that gives details about each object. A directory is a specialized database that differs from general-purpose relational databases in that a directory is (usually) accessed much more often that it is updated. Directories are usually accessed using the client/server model of communication. Of course, for a directory service to work on a network, the format and content of the directory-related messages exchanged between the client and server must adhere to an agreed upon protocol.

Directory client/server interaction is illustrated in Figure 2.4-6.

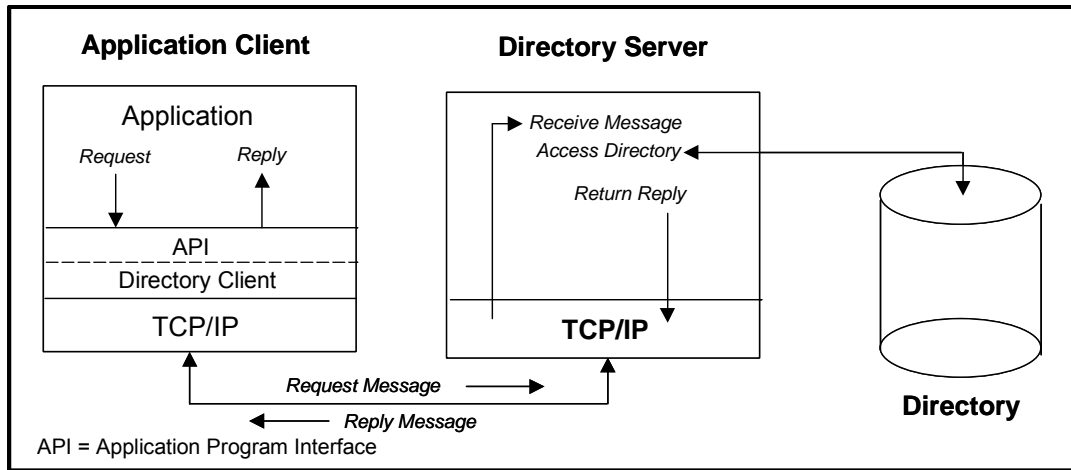


Figure 2.4-6: Directory Client/Server Interaction

2.4.5.2 Characterizations

In the world of directory services there are several ways to characterize directories. These include:

- Scope of information
 - Local
 - Global
- Location of clients
 - Local
 - Global
- Distribution of servers
 - Centralized
 - Distributed
 - Partitioned
 - Replicated

These three “dimensions” of a directory: scope of information, location of clients, and distribution of servers are independent of each other, so that directories may be characterized in many combinations of these three dimensions.

A major consideration of directory services is the required security of the information stored in a directory. Robust directory service standards provide methods to maintain applicable levels of security.

2.4.5.3 Need for Common Directories

If every part of an enterprise was an informational island, then each could have its own proprietary directory service. Of course, this is not the case for distributed systems, whose constituent components have to interface with each other. This suggests a need for standards-based common directory structures. As a matter of fact, it can be advantageous to consider common directories as part of the system infrastructure for the following reasons:

- A common (standardized) directory accessible by all applications is a vital part of the infrastructure supporting a distributed system.
- A common directory service provides a single logical view of the users, resources, and other objects comprising a distributed system.
- Users and applications can thus access network resources transparently, and the system is perceived as an integrated whole, not a collection of independent parts.

Given the viewpoint of common directories as infrastructure, it can further be seen that there are several benefits of employing common directories in a network, including the following:

- They are based on an open standard supported by many vendors on many platforms.
- They are accessible through a standard application programming interface (API).
- They are robust.
- They can be made to be secure.
- They are scalable.

2.4.5.4 Network Directory Service Standards

Several network directory service standards have evolved over the last decade and a half. In 1988, the CCITT (now ITU-T) created X.500 (*ISO 9595, Data Communications Network Directory, Recommendations X.500-X.521*). This standard is based on the Open Systems Interconnection (OSI) protocol stack and organizes directory entries in a hierarchal name space capable of supporting large amounts of information. It also defines powerful search capabilities to make retrieving information easy for a large mainframe based enterprise. X.500 specifies that communications between directory client and directory server uses the directory access protocol (DAP). However, it is well known that supporting the full OSI protocol stack requires more resources than usually available in small environments, and furthermore it's not employed in today's ubiquitous IP-based networks. For this reason, other protocols are needed.

Thus the lightweight directory access protocol (LDAP) was developed. LDAP uses the "lighter weight" and more popular TCP/IP protocol stack instead of OSI. It has evolved over the years after originally being an offshoot of X.500. LDAP (version 1) was first defined in RFC 1777 issued by the IETF. RFC 1777, along with several other later RFCs, define LDAP Version 2, which has reached the status of draft

IETF standard. LDAP Version 3, defined in RFC 2251 and which extends LDAP Version 2, is a proposed standard.

3. COMPARATIVE ANALYSIS OF FAA COMMUNICATIONS SERVICE NEEDS VS. AVAILABLE SERVICES AND TECHNOLOGIES

Section 2 discussed the technological methods for achieving high QoS levels of communications service. This section discusses the service needs of the FAA and compares these needs with the performance of current commercial wide area network services and technologies. This comparison is discussed in four categories as follows:

- Data Delivery Service.
- Voice and Videoconferencing.
- Security.
- Enterprise Management.

3.1 DATA DELIVERY SERVICES

Data Delivery service is specified by the basic QoS performance parameters of bandwidth, data latency, availability, and packet data loss. Each of these is discussed below in the context of FAA needs.

3.1.1 FAA Needs

3.1.1.1 Bandwidth

An analysis of FAA communications requirements for bandwidth on a previous study¹⁵ indicates that the large majority of data traffic falls into two major categories:

- Communications between major FAA centers: Air Route Traffic Control Center (ARTCC) to ARTCC and ARTCC to Terminal Radar Approach Control Facility (TRACON).
- Communications between major FAA centers and small widely-scattered sites: Remote Communications Air/Ground Facilities (RCAGs), Backup Emergency Communications (BUECs), Air Route Surveillance Radars (ARSRs) that surround that center (ARTCC or large TRACON).

The overall bandwidth requirement for the first category is typically several Megabits per second (Mbps). The bandwidth requirement for the second category is dependent upon whether the site supports voice communications. Where voice circuits are required, two to four voice circuits are typical. Assuming a conversion of each voice circuit to a data rate of 64 kbps yields an overall requirement on the order of 256 kbps. Where voice circuits are not involved, the data rate requirements are low (typically below 64 kbps).

3.1.1.2 Availability

FAA's end-to-end performance goals for service availability are stated in NAS-SR-1000. Table 3.1-1 contains those performance goals for three defined categories: critical, essential, and routine. In addition to the availability parameter, the table lists the maximum tolerable restoration times and minimum time between outages for each of the service types. It is important to note that the values are end-to-end service availability of which communications is just one component. Thus, the performance values for communications availability should exceed those of Table 3.1-1.

NAS Service Category	Availability	Maximum Restoration Times	Minimum Time Between Outages
Critical	0.99999	6 seconds	One week
Essential	0.999	10 minutes	One week
Routine	0.99	1.68 hours	One week

Table 3.1-1: FAA's Goals for Service Availability

3.1.1.3 Latency

The NAS-SS-1000 Volume I (pg. 58) specifies an overall latency for critical surveillance data. The allowed latency from the ARSR-9 and ARSR-11 to the display is 2.2 seconds, but the amount allocated to the communications is 0.3 seconds (300 msec). For simplicity, since such surveillance data is classified as critical, this latency has been applied to all FAA critical data, as indicated in Table 3.1-2. The NAS-SR-1000 Volume 4 (pg. 3-152) specifies latencies of 600 msec to 10 seconds, depending upon the service, and these values have been inserted in Table 3.1-2.

NAS Service Category	Latency
Critical	< 300 msec
Essential and Routine	600 msec – 10 secs

Table 3.1-2: FAA Goals for Data Latency Due to Communications

3.1.1.4 Packet Loss

There is no FAA document that articulates a tolerable percentage of data loss. Packet loss results in the loss of data only when a real-time data stream is sent without a "reliable" delivery protocol (e.g., TCP). Thus it is only applicable to real-time data streams such as radar data. A "worst case" tolerance for packet loss can be inferred from FAA's tolerance for outages for critical radar data: a 6 second loss of data over a week represents a 99.999% availability and this can be translated into a tolerance of 0.001 % packet loss.

3.1.2 Delivered Performance of Commercial Data Delivery Services

3.1.2.1 Overview of Communications via Packet Networks

When point-to-point leased lines are used to deliver high-speed data telecommunications service, the desired communications performance is achieved by ordering a sufficient number of lines with sufficient bandwidth to support a known amount of data traffic. The availability performance is similarly met by ordering reliable and backup redundant lines. By moving telecommunications services to a shared network, critical network performance factors are no longer guaranteed by dedicating a specific set of resources. In this environment, network service providers offer Service Level Agreements (SLAs) to assure customers that their managed network will achieve the necessary performance.

The SLA is the basis for specifying the QoS of a defined service within a modern communications network. The SLA is a contract between the user and service provider for a specified QoS. SLAs are comprehensive, covering not only the QoS parameters of basic data delivery service (bandwidth, availability, data latency, and packet loss), but also the interface to the service, as well as value-added services such as voice, video conferencing, security, and enterprise management applications.

In support of this study, a survey of network service provider SLAs was conducted to understand what QoS levels were available and to compare that with FAA needs to assess their suitability. Samples of the SLAs being offered by backbone network communications service providers were collected to determine what basic and value-added service guarantees were being made. Some large network providers post simple SLAs on the Internet. Several more SLAs were obtained from providers' service representatives. Individual SLA contracts can be negotiated and may be very comprehensive and complex. However, company-proprietary SLAs were not available for analysis, so the focus of the SLA survey was on the QoS parameters of basic data delivery service.

Table 3.1-3 lists the availability and data delay QoS parameters of Frame Relay services offered by major communications network service providers. We focused on Frame Relay because it is a mature technology that is offered by all major service providers and thus supplied a solid picture of its readily obtainable service performance. However, ATM and IP networks provide similar performance. In particular, as IP technology and its associated protocols mature, a richer variety of QoS will be offered over IP networks at low cost, and emerging technologies for bandwidth reservation allocation and network traffic management are expected to enable the offering of even higher QoS levels.

It is important to note that the values in Table 3.1-3 are typically exceeded by the service providers. Ongoing monitoring of the performance parameters by the service provider supports service assurance, and failure to meet a performance parameter over a defined period of time results in a sizeable discount in the service fee over that period of time. In all the SLAs studied economic relief is offered to customers when monitored measurements indicate that the guaranteed service levels are not met. While no customer is likely to look forward to receiving rebates at the cost of loss of service, the penalties in these contracts help to ensure that the networks have been engineered to exceed the promised requirements to avoid

compromising their revenues. Moreover, the measurements, such as average monthly network availability and average round-trip network delay, which are collected to monitor the performance of the service with respect to SLA parameters, produce a record of performance over time. Some independent concerns even post the large carriers' performance records on the Internet. Existence of these historical records increases the incentive for service providers to do everything possible to meet their promises. A provider's good record diminishes risk for prospective users, such as the FAA, that require a high-performance QoS.

Frame Relay Network Service Providers and Their Service Guarantees							
	AT&T	Intermedia	Qwest	Qwest	MCI/Worldcom	Sprint	Sprint
			real time PVCs	non real time PVCs		Voice/SNA PVCs	LAN PVCs
Network Availability							
Average Network Availability		99.98%					
Customer end-to-end		99.95%	99.50%	99.50%	99.80%	99.90%	99.90%
Customer end-to-end, w/carrier access link						100.00%	100.00%
Carrier POP to POP	99.99%	99.99%	100.00%	100.00%	100.00%	100.00%	100.00%
Network Transit Delay		Frames of < 256 bytes			Frames of < 200 bytes		
Customer 1-way end-to-end		85 ms			60 ms	50-115 ms	70-130 ms
Carrier 1-way POP to POP delay	60 ms	60 ms	15-60 ms	15-60 ms			
Frame Delivery Rate							
Within CIR, End-to-End		99.90%					
Within CIR, POP-to-POP	99.99%	99.99%	99.99%	99.90%	99.99%	99.90%	99.90%
Above CIR, End-to-End		99.00%					
Above CIR, POP-to-POP		99.50%		99.50%		99.00%	99.00%
MTTR (PVC or port maintenance)	< 4 hours	< 4 hours	< 4 hours	< 4 hours	< 2 or 4 hours	< 4 hours	< 4 hours
Number of POPs	600		507	507	700 (incl. ATM)		

Table 3.1-3: QoS Parameters of Frame Relay Service Offered by Major Providers

The availability QoS parameters in the table require some description. "Network Availability" refers to the percentage of time the network provides connectivity, but not necessarily with the desired bandwidth. The "Within CIR" parameter refers to the percentage of time that the Committed Information Rates (CIR) bandwidth specified in the SLA is provided. Note that it tends to be lower than the "Network Availability." To understand the difference between Point of Presence (POP) to POP and end-to-end availability, in the above table it is instructive to examine the picture of a packet communications network shown in Figure 3.1-1. This figure shows communications between FAA Facility A and FAA Facility B via a Network. To access the services of the Network, an FAA Facility must lease an access line to a Point of Presence (POP) on the Network. A POP is typically a major switching node on a service provider's network. At a minimum, a POP contains a switch that houses an interface card that supports an input port that matches the communications protocols used by the access line. As illustrated in Figure 3.1-1, end-to-end communications between Facility A and Facility B is composed of three parts:

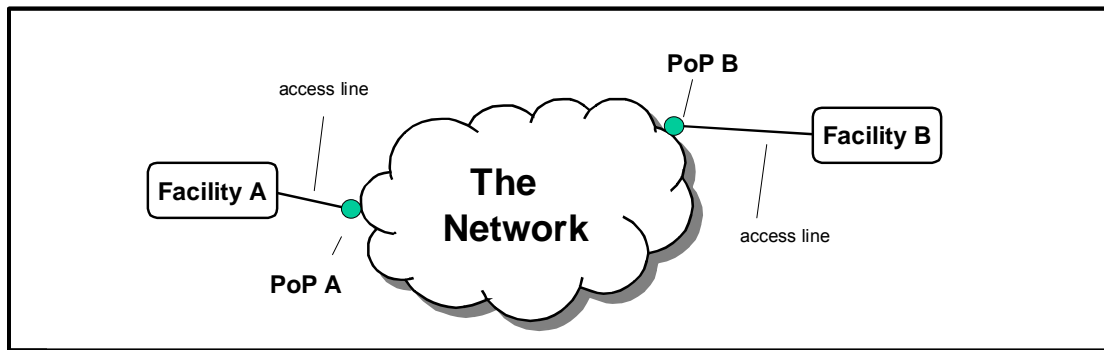


Figure 3.1-1: Illustration of POPs and Access Lines for Network Service

- Access communications between FAA Facility A and its POP: this is provided by a dedicated set of resources, which may or may not be redundant depending upon its availability requirements.
- POP to POP communications over the Network “Cloud”: the POP-POP connectivity is provided by the overall resources of the network; this connectivity is highly redundant and therefore extremely reliable. Also, because of the sharing of resources over the network, reliable communications can be provided efficiently and cost-effectively.
- Access communications between FAA Facility B and its POP: this is provided by a dedicated set of resources, which may or may not be redundant depending upon its availability requirements.

Figure 3.1-2 illustrates an example of the Network Cloud provided by an IP network of AT&T built upon a transcontinental backbone of OC-48 links. Close examination indicates it is built upon SONET lines from OC-3 up to OC-192. Upgrades of the backbone to OC-192 are also taking place.

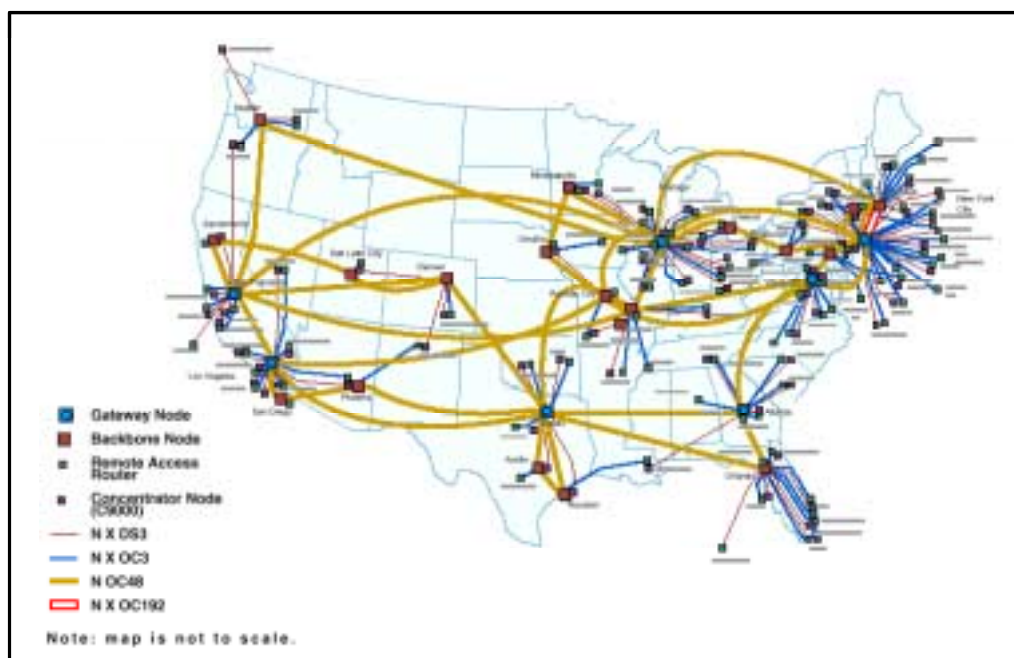


Figure 3.1-2: Example Structure of Network Cloud (AT&T IP Network)

3.1.2.2 Bandwidth Over a Packet Network

The bandwidth between Facility A and Facility B will be determined by the size of the access lines and the bandwidth available to the data traffic between A and B on the Network. Frame Relay and other packet services allow Permanent Virtual Circuits (PVCs) to be set up through the Network (from POP to POP) to support data traffic, but there are many other alternatives for bandwidth reservation as well. Many virtual circuits may be supported from a single facility, but the access line needs to be sized to contain them all. The Frame Relay protocol supports data rates from 56 kbps up to 45 Mbps, and higher data rates are supported within an ATM or other high-speed core of the Network. Access to a Frame Relay network is achieved via dedicated link between the facility and a POP. Where that link is a wired terrestrial link, the leased access line can be as small as a DS0 or as large as a DS3. Conversion to Frame Relay occurs at the facility via a Frame Relay Access Device (FRAD). The access may also be supported via emerging broadband wired (e.g., DSL) and wireless (e.g., Multichannel Multipoint Distribution Service (MMDS)/Local Multipoint Distribution Service (LMDS) or satellite) access technologies.

3.1.2.3 Availability Over a Packet Network

As indicated in Table 3.1-3, POP-POP communications is very reliable: 99.99% availability at a minimum, with some offering 100.00%. The weak links in the availability chain are the access lines to the POPs. As shown in the above Table 3.1-3, the major providers of Frame Relay networks have POPs in continental US that number up to several hundred. However, they tend to be concentrated in major metropolitan regions. Thus, while FAA's major facilities (ARTCCs and large TRACONS) will be close to a POP of a network service provider, other facilities will often be far from a POP. For FAA facilities that are close to a POP, the service provider will typically support access that provides POP presence and the associated excellent reliability at the facility. For FAA facilities that are remote from a POP, the end-to-end communications performance will tend to be dominated by the access communications. Thus the issue of choosing the best access technology to the Network is an important one.

3.1.2.4 Data Delay Over a Packet Network

As indicated in Table 3.1-3, data delay over a packet network is a variable, but it can be controlled within a desired tolerance. As in the discussion of availability, there is a distinction to be made between end-to-end delay and POP-POP delay. For the networks listed, the 1-way delay for POP-POP communications is always < 60 msec. For end-to-end communications, the delays in the SLAs tend to be somewhat higher: up to a maximum of 130 msec. Figure 3.1-3 illustrates that the average data delay experienced depends upon the locations within the network. An analysis would reveal that one of the major determinants of delay is the number of routers between the two points, and for that reason, the delay is somewhat proportional to distance. Note that for nearby locations, the data delay is low (e.g., Washington-Atlanta is 17 msec), and for far apart locations, the data delay is high (e.g., Washington-Seattle is 70 msec).

CITY PAIRS	Atl																			
Cambridge	28	Cam																		
Chicago	35	25	Chi																	
Dallas	16	45	21	Dal																
Denver	36	65	42	22	Den															
Los Angeles	51	70	49	38	33	LA														
New York	23	20	19	55	58	66	NY													
Orlando	11	37	44	25	45	60	46	Orl												
San Francisco	72	64	41	46	25	10	58	68	SF											
St. Louis	33	40	17	15	36	42	43	42	41	StL										
Seattle	80	70	47	66	41	25	64	89	17	57	Sea									
Washington	17	13	25	30	51	57	30	25	57	18	70									

Current Overall Average: 41 ms

Figure 3.1-3: Data Delay Over a Network

3.1.3 Comparison of FAA Needs with Available Packet Services

3.1.3.1 Bandwidth

The service bandwidth offered by major packet communications service providers far exceeds the requirements of FAA's NAS. As introduced above, we consider the two types of NAS communications requirements:

- Communications Between Major Facilities: major facilities are near POPs and so have access to the OC-48 backbone, which far exceeds the FAA's needs, which is on the order several DS1 lines. Indeed, the NAS communications bandwidth requirements can be satisfied within the current bounds of Frame Relay alone, which supports bandwidth up to DS3.
- Communications Between Small/Remote Facilities and Major Facilities: as indicated earlier, the bandwidth requirements in this category are met by as little as a single DS0 circuit, but, at sites that support operational voice communications (e.g., RCAGs), multiple DS0 circuits are required. Clearly, the same lines that currently support circuit communications with these sites may be used as access lines to a packet network. In addition, the use of packet protocols easily accommodates the multiplexing of multiple data stream on a single link. This allows a wider variety of wired access circuits (including fractional DS1, DSL and cable) and wireless access circuits (including MMDS/LMDS and next generation cellular and satellite data communications).

3.1.3.2 Availability

For some aspects of the NAS communications requirements, the service availability offered by major packet communications service providers comes close to or meets the requirements of FAA's NAS. As introduced above, we consider the two types of NAS communications requirements:

- **Communications Between Major Facilities:** major facilities are near POPs and so the communications between major facilities can be supported with the POP-POP availabilities. The reported range supported by the service providers is 99.99% - 100%. These values are certainly adequate for essential and routine communications. However, for critical communications, which requires better than 99.999% connectivity, only the networks that support 100% availability in the SLA meet the requirements of the NAS. Thus, it appears that the highest quality current commercial offerings can support the NAS communications availability requirement between major facilities.
- **Communications Between Small/Remote Facilities and Major Facilities:** because the availability of this type of communications requires an access link, the end-to-end availability parameter of the networks varies from 99.8% to 99.95 %. This range is adequate for routine communications, but only the higher end can support essential communications. Furthermore, the range does not support critical communications with its > 99.999% requirement. Clearly, to meet the requirement for critical communications, redundant access links will need to be implemented, much as redundant links are currently implemented for point-to-point circuit communications within the NAS. This may be implemented as two independent links over the same media type (e.g., two DS0 links) or may be two dissimilar links (on DS0 link and a satellite backup link).

3.1.3.3 Data Delay

For all aspects of the NAS communications requirements data delivery, the data delay performance of current networks is more than adequate. In all the data presented above, the achieved data delay was significantly less than the 300 msec requirement cited for critical radar data.

3.2 VOICE/VIDEO

3.2.1 FAA Service Needs

3.2.1.1 Voice

The FAA requirements for voice services are typically expressed in terms of latency and availability.

3.2.1.1.1 Availability

The FAA requirements for voice circuit availability are clear, and quantifiable when discussing leased lines. If voice communications services are delivered over packet switched networks, additional considerations will be entailed. Specifically, a fundamental definition must be made as to what comprises a failure. In other words, a process must possess two states: “ON” and “OFF” to be quantified in the availability calculation. The “ON” state, and “OFF” states are used to determine the meaning of the Mean Time to Failure (MTTF) and Mean Time to Repair (MTTR) in the availability calculation:

$$A = \frac{MTTF}{MTTF + MTTR}$$

In a circuit switched network, the “ON” state is easy to quantify. To be “ON”, voice circuits are expected to be clean (i.e., high signal-to-noise ratio) and echo-free. Defining the “ON” state for packet switched

network should take into account periods of time when the delivered performance falls below the required performance. With digital voice services, a set of metrics can be defined that closely follow circuit quality. These metrics, and acceptable ranges for them are discussed in the sections describing the delivered performance of available services.

3.2.1.1.2 Latency

One effect of latency is that excessive end-to-end delay makes conversation inconvenient and unnatural. ITU-T G.114 recommends 150 ms as the maximum desired one-way latency to achieve high quality voice. Figure 3.2-1 presents the results of subjective tests to measure voice quality as a function of pure delay. A distinction is made here between delay and echo. In Figure 3.2-1, reference is made to the Mean Opinion Score (MOS). This is a subjective measure used to quantify ease of communications and perceived voice quality. In this method, listeners rate the speech under test on a five-point scale where a listener's subjective impressions are assigned a numerical value (between 1 and 5, 1 being the worst, 5 the best). A MOS of 4.0 or greater is referred to as toll quality¹⁶.

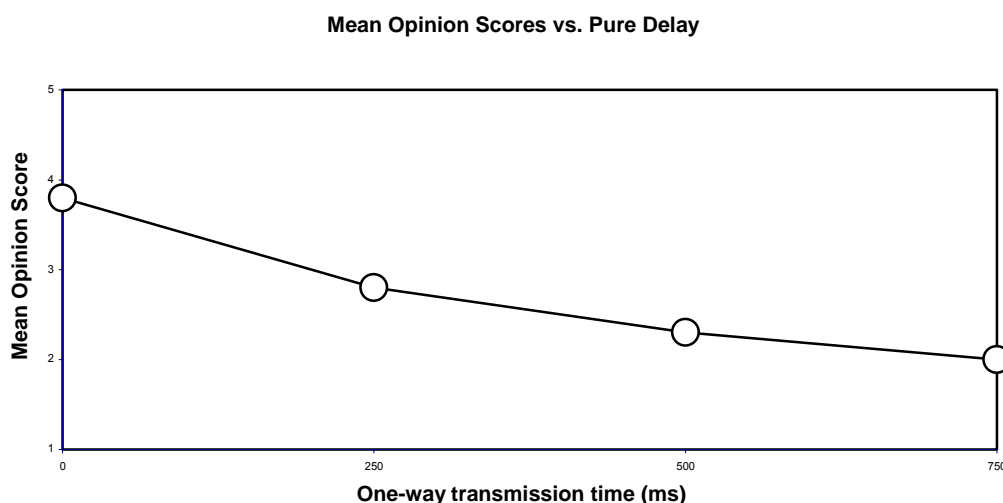


Figure 3.2-1: Subjective Evaluation of Speech Quality as a Function of Pure Delay¹⁷

ITU-T recommends the limits provided in Table 3.2-1 for one-way transmission time for connections with echo adequately controlled.

Table 3.2-1: ITU-T Recommendations for Maximum One-Way Delays

Delay Range	Application
0 to 150 ms	Acceptable for most user applications
150 to 400 ms	Acceptable provided that administrations are aware of the transmission time impact on the transmission quality of user applications
Above 400 ms	Unacceptable for general network planning purposes; however, it is recognized that in some exceptional cases this limit will be exceeded

A latency requirement that is frequently quoted from the NAS SR-1000 is: “Initiation of one-way air-ground voice transmissions shall be possible within 250 milliseconds of keying the specialist’s microphone”¹⁸. Therefore, a design goal for voice communications should be 150 ms end-to-end delay, with a requirement of no more than 250 ms.

3.2.2 Delivered Performance of Available Services

The delivered performance of voice-over-packet is a function of

- Dropped Packets
- Latency
- Echo
- Jitter Buffering
- Vocoder Selection

3.2.2.1 Dropped Packets

Dropped packets usually result in the loss of transmitted information. This can be compensated for by either of the following:

- Interpolating for lost packets by replaying the last received packet.
- Sending redundant information.

However, studies have shown that VoIP voice quality is relatively tolerant to packet loss. Figure 3.2-2 provides the results of a recent study.

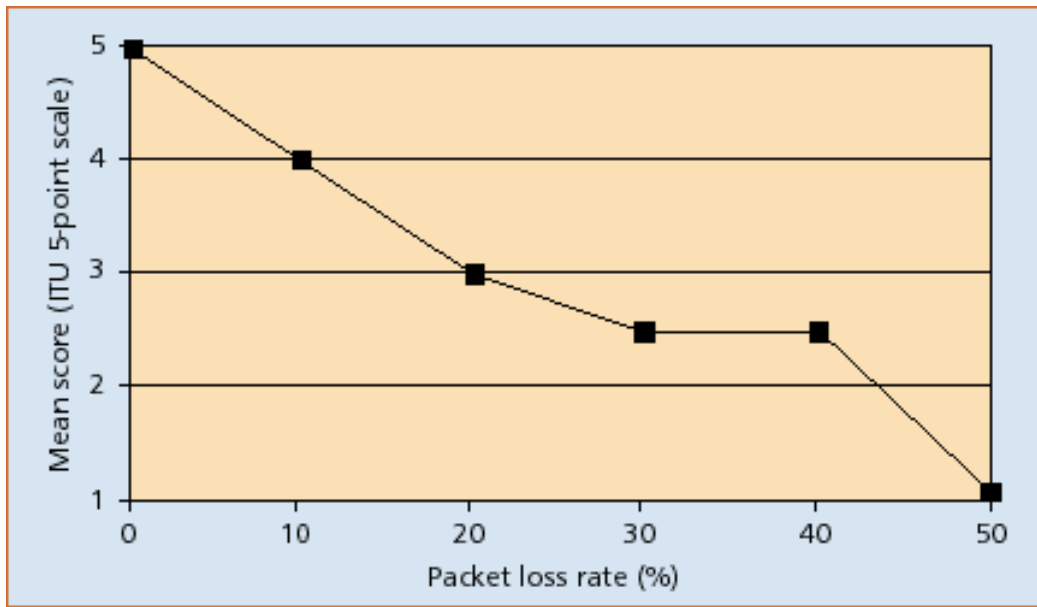


Figure 3.2-2: Voice Quality as a Function of Packet Loss Rate¹⁹

3.2.2.2 Latency

3.2.2.2.1 Latency Sources

Sources of latency (delay) for a VoIP call include the following:

- Coding and Decoding Delay
- Serialization Delay
- Queuing Delay
- Propagation Delay
- Jitter Buffer

The first four of these sources will be discussed in the following sections. Jitter Buffering will be described in Section 3.2.2.4.

3.2.2.2.1.1 Coding and Decoding Delay

Analog–digital conversion and voice compression introduce delays in the codec (see Table 3.2-2). The low rate vocoders can be thought to operate on the output of a PCM (G.711) vocoder. Hence the delay terms in this table are meant to be delays in addition to the G.711 delays. For example, CS-ACELP (ITU G.729 standard) requires input samples that are either 16 bit linear samples or 8 bit μ -law/A-law encoded data (in other words the output of a G.711 vocoder).

Table 3.2-2: Codec Standards and Associated Delays^{20 21}

Coding Standard	Compression Algorithm	Compression Algorithm Bit Rate (kb/s)	Frame Processing Delay (ms)	Lookahead Delay (ms)	Total Encoding Delay (ms)	Typical Decoding Delay (ms)	Typical End-to-End Delay (ms)	Equipment Impairment Factor (Ie)
G.711	PCM	64	N/A	N/A	<1	<1	<1	0
G.728	LD-CELP	16	N/A	N/A	<2	<2	<2	7
G.729	CS-ACELP	8	10	5	15	7.5	22-35	12
G.729A	CS-ACELP	8	10	5	15	7.5	22-35	13
G.723.1	ACLEP	5.3	30	7.5	37.5	18.75	55-97	19
Note 1: PCM = Pulse Code Modulation, ACELP = Adaptive Code-Excited Linear Prediction, and CS-ACELP = Conjugate Structure ACELP								
Note 2: All delays are one-way.								
Note 3: Ie values are in accordance with ITU Recommendation G.113, Appendix I.								

Higher compression is achieved at the price of longer delays. Two factors that contribute to the total encoding and decoding delay are frame processing delay and lookahead delay. The "Framing Delay" in the table refers to the accumulation of buffer delay. This buffer is required to accumulate enough speech samples to make filter coefficient estimates, pitch estimates and the like. The "Look-Ahead Delay" is the delay to process part of the next frame to exploit any correlation in successive voice frames.

3.2.2.2.1.2 Serialization Delay

Serialization delay is the time it takes to place a packet on the transmission line. This delay is determined by the speed of the line; for instance, it takes 125 μ s to place 1 byte of information on a 64 kb/s line. Table 3.2-3 shows the resultant delay for accessing a 64 kb/s line for various packet types.

Table 3.2-3: Packet Serialization Delay for Compressed and Uncompressed Headers of Two Recommended Vocoders

Packet Type	Packet Size	Serialization Delay
Compressed header G.723.1 packets	28 bytes	3.5 ms
Uncompressed header G.723.1 packets	64 bytes	8 ms
Compressed header G.729 packets	14 bytes	1.75 ms
Uncompressed header G.729 packets	50 bytes	6.25 ms

3.2.2.2.1.3 Queuing Delay

Queuing Delay occurs at the various switching and transmission points of the network, such as routers and gateways, where voice packets wait behind other packets waiting to be transmitted over the same outgoing link. A useful rule of thumb is that each router introduces 10 ms of delay. Queuing delays can be reduced by using faster links or by prioritizing voice packets over data packets. Protocols that can be used for prioritizing voice packets include DiffServ and RSVP. The effect of increasing link speed on queuing delay is shown in Figure 3.2-3.

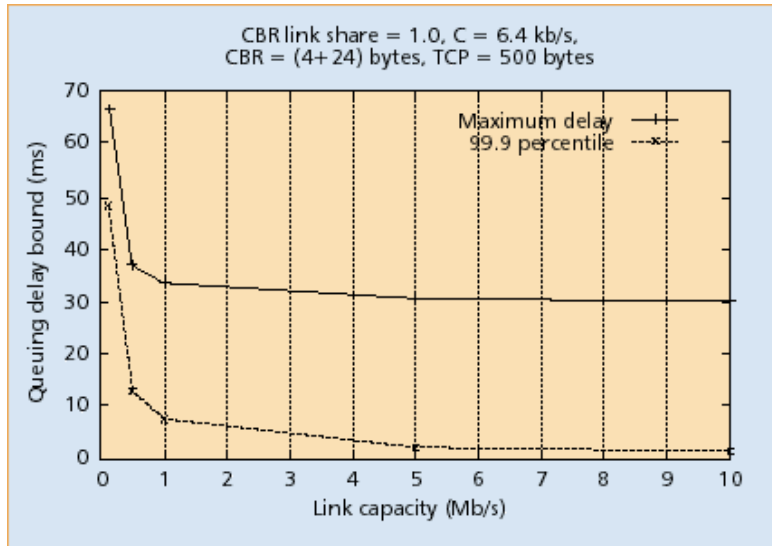


Figure 3.2-3: The Impact of Link Capacity on Queuing Delay²²

In the simulation that produced Figure 3.2-3, data packets (labeled TCP in the figure header) had a uniform size of 500 bytes, and voice packets (labeled CBR in the figure header) consisted of a data payload of 24 bytes and a compressed header of 4 bytes. The committed link share to voice packets in this simulation was one (this is the worst case scenario, i.e., corresponds to the most delay, as can be seen from Figure 3.2-4), so that a T1 link supported 205 voice streams. It is clear from the figure that the delay time decreases as the link capacity increases. The 99.9 percentile delay bound decreases to about 3 ms for a link of more than 5 Mb/s, indicating that the queuing delay of voice packets is negligible from a practical point of view when a link is more than 5 Mb/s.

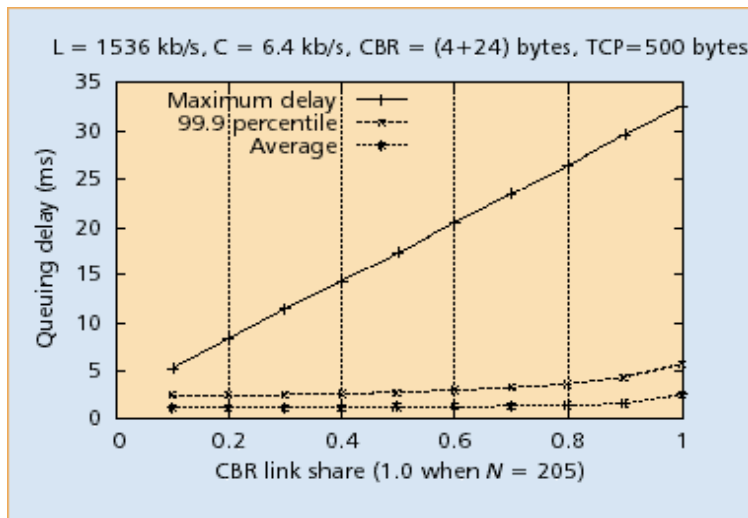


Figure 3.2-4: The Impact of Constant Bit Rate (CBR) Link Sharing on Queuing²³

3.2.2.2.1.4 Propagation Delay

Propagation Delay is the time required by signals to travel from one point to another. In telecommunications circuits, a rule of thumb is that the propagation delay is roughly 1 ms per 250 km (taken from ITU G.114).

3.2.2.2.2 Latency Mitigation Techniques

Two technologies to reduce delay have been proposed by the IETF: 1) compression of the header on voice packets, and 2) segmentation of other traffic on the shared network.

3.2.2.2.2.1 Header Compression

This technique reduces each voice packet's overhead, leading to efficient use of network resources such as intermediate routers and links. Header compression is particularly effective for low-bit-rate voice codecs. For example (refer to Figure 3.2-5), the G.723.1 codec generates a frame of 24 bytes at intervals of 30 ms. Each frame is conveyed with the payload of an IP packet, typically 40 bytes in IPv4. This results in inefficient use of network resources. The header size can be reduced to 2 bytes without header cyclic redundancy check (CRC) or four bytes with CRC by use of compression schemes.

3.2.2.2.2.2 Segmentation of other Traffic on a Shared Network

This technique is applied to TCP packets sharing network resources with voice packets, decreasing TCP packet transmission time and in turn decreasing the waiting time of voice packets. When used with prioritization (QoS) protocols, this is especially effective. Without segmentation, even if voice packets have priority over non-real-time packets, they will be forced to wait until the transmission of non-real-time packets currently being served ends. Therefore, large non-real-time packets or TCP packets should be segmented. This enables voice packets to be interleaved with segmented TCP packets of small size, resulting in small waiting times for voice packets.

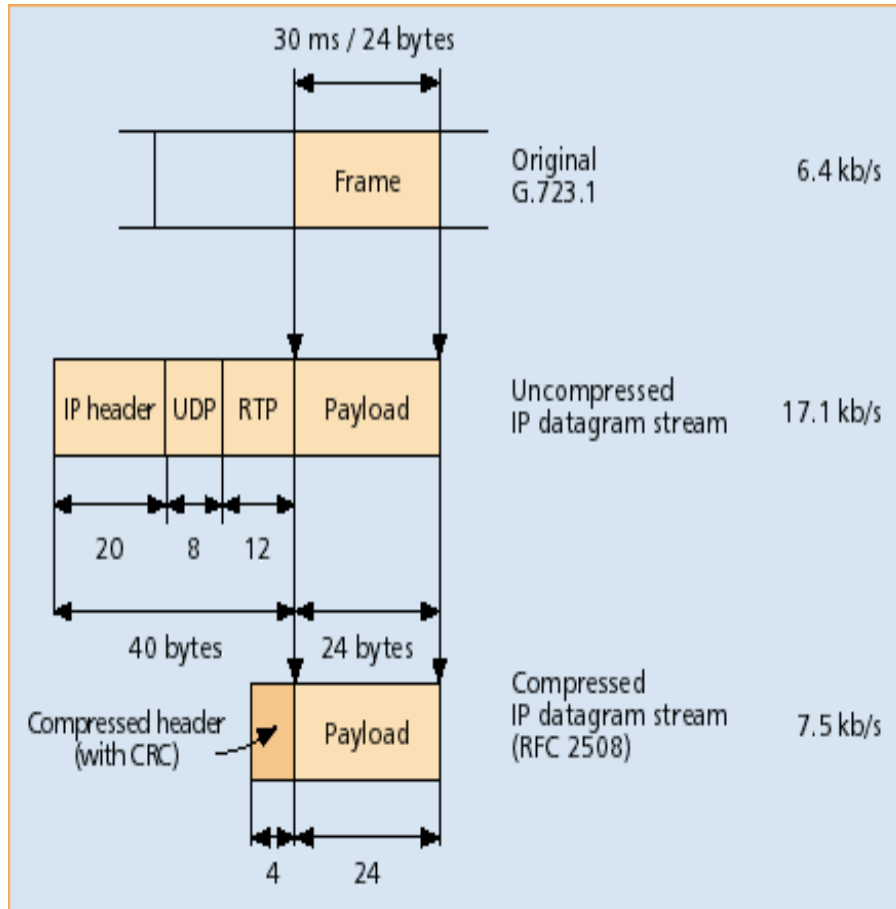


Figure 3.2-5: Encapsulation of Vocoder Packet, Showing Overhead With and Without Header Compression

Figure 3.2-6 shows the impact of decreasing header size on queuing delay. A careful consideration of Figures 3.2-3, 3.2-4, and 3.2-6 indicates that a router latency on the order of 5 ms can be expected when trunk capacity is greater than 1.5 Mbps, if traffic shaping is used and header compression is employed.

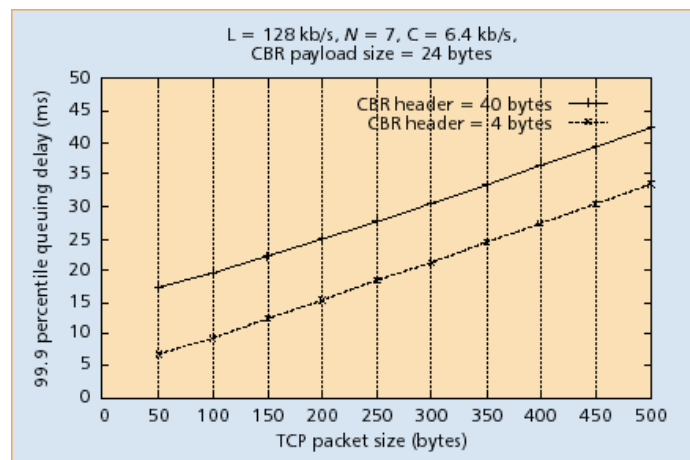


Figure 3.2-6: Impact of Header Overhead on the 99.9 Percentile Delay Bound²⁴

3.2.2.2.3 Typical VoIP Latency Performance

Table 3.2-4 shows representative values for the various delay components of VoIP, resulting in a nominal delay budget of 150 ms. Figure 3.2-7 shows measured results for end-to-end implementations of various vendor products. All of the tested products in Figure 3.2-7 have end-to-end latencies less than or equal to 150 ms.

Table 3.2-4: VoIP Delay Budget

Delay Component	Value	Justification
Coding Delay	15 ms	Use of a G.729 vocoder
Serialization Delay	1.75 ms	Upper bound for compressed header G.729 packets on a 64 kbps line
Propagation Delay	1 ms	250 km transmission distance
Queuing Delay	20 ms - Or - 25 ms	2 router hops, 10 ms/hop from rule of thumb - Or - 5 router hops, 5 ms/hop from analysis
Jitter Buffer	100 ms	Design Decision
Decoding Delay	7.5 ms	Use of a G.729 vocoder
Total	150.25 ms	

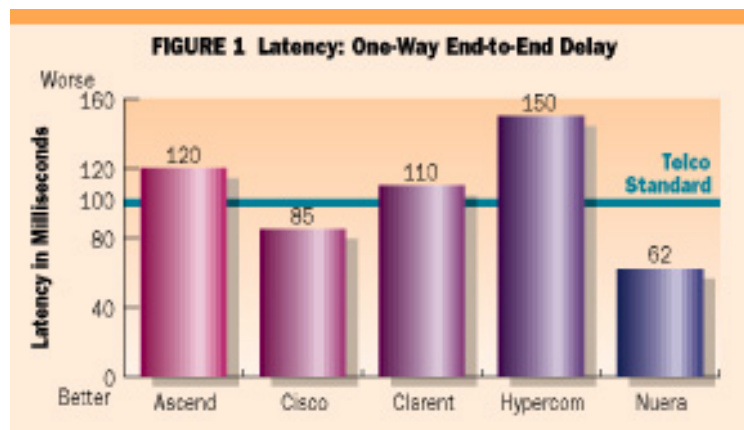


Figure 3.2-7: Measured End-to-End Latency Values for Various VoIP Implementations²⁵

3.2.2.3 Echo

The degree to which echo is objectionable depends on echo loudness and total delay. If the delay is small (less than 10 or 20 ms), the listener hears either nothing or a reverberant sounding side-tone at most. Larger delays lead to a subjective annoyance perceived as echo. The larger the delay, the less masking there is by the direct speech and the more annoying the echo is.

Figure 3.2-8, from ITU-T G.131 (control of talker echo), shows the variation in acceptable perceived echo loudness versus total delay, where:

$$TEL R = SLR + RLR + R + T + Lr$$

TELR = talker echo loudness

SLR = speaker loudness rating = 7dB nominal, 2dB minimum for most telephones

RLR = receiver loudness rating = 3 dB nominal, 1 dB minimum for most telephones

R = receive loss

T = transmit loss (R+T = 6 dB is introduced in most calls in the US for echo control)

Lr = return loss or hybrid balance = 14 dB nominal, 8 dB minimum for line cards that subtract a constant fraction of the signal being sent due to the variation in telephone and loop impedance.

Adding all of these variations gives a 17 dB minimum TELR and 30 dB nominal. The worst case TELR of 17 dB would be objectionable for most subscribers at 8 ms of delay, and objectionable to some subscribers at less than 5-ms delay. The average TELR of 30 dB would be objectionable to most subscribers at 35 ms of delay, and could be objectionable to some subscribers at 18 ms of delay.²⁶ In the case of long delays (for example, more than 20 ms), better echo performance is required (over 35 dB of ERL). Some long delay examples are long distance calls over 1,000 km, VoIP, voice over Ethernet, and wireless local calls. In these situations, fixed hybrid balance with loop segregation generally provides unacceptable performance and echo cancellation at the line-card level or network echo cancellation is required.

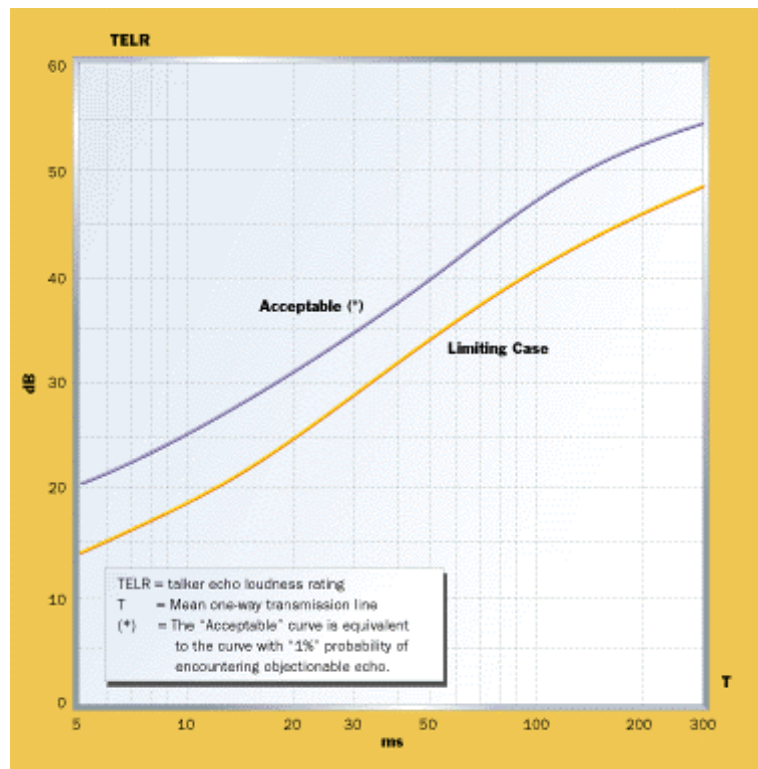


Figure 3.2-8: Required Echo Suppression as a Function of Absolute Delay²⁷

3.2.2.4 Jitter Buffering

Variance in the interframe arrival times at the receiver is called *jitter* and is potentially more disruptive for IP telephony than latency alone. Jitter occurs due to the variability of queuing delays in the network. One strategy for handling the inherent packet delay of a packet network is to use a jitter buffer. Upon initiating a conversation, the VoIP device fills the jitter buffer with packets, creating an initial delay in the conversation. At this point, the jitter buffer can protect a system against packets that are delayed, because reserve packets in the buffer can play until the delayed packets arrive. The jitter buffer also protects against packets that arrive out of order; when an out-of-order packet finally arrives, the controller opens the appropriate place in the buffer and inserts the packet.

The jitter buffer effectively allows continuous playing of voice data, even when packets are lost or damaged. When packets are lost (that is, the packets don't arrive in time to be useful), the buffer shrinks. A system controller judiciously adding comfort-noise packets (white noise that worries a listener less than complete "is-my-phone-dead?" silence) may cover the loss of a few packets without a listener noticing. The controller can also repeat the previous packet, but this strategy is most effective with silence or low-pitched voice packets of 10 msec; a listener might notice if a packet repeats more than once, or if a longer packet repeats.

3.2.2.5 Vocoder Selection

Intelligibility is mainly determined by the choice of the vocoder, the device that converts analog voice signals into digital signals and then convert them back into speech sounds²⁸.

Three of the more common vocoders are those described by the ITU-T standards, G.711, G.723.1, and G.729A. The key points of these vocoders are briefly described below.

- **G.711:** The G.711 algorithm encodes non-compressed speech streams running at 64 Kbps. This is toll-quality speech, equivalent to voice on the PSTN network, and requires the full-bandwidth of traditional circuit-switched voice channels.
- **ITU G.723.1:** This International Telecommunications Union (ITU) algorithm runs at 6.4 or 5.3 Kbps and uses linear predictive coding and dictionaries, which help provide smoothing. The smoothing process is CPU-intensive, however (30 Million Instructions Per Second (MIPS) on an Intel Pentium), which means that a scalable solution requires substantial computing power. Among ITU speech encoders, G.723.1 delivers toll-quality performance at the lowest bit rate. It also specifies the generation of comfort noise frames during silence periods, which greatly enhances the perceived quality of speech. G.723.1 has been chosen as the default speech encoder for IP telephony by the International Multimedia Teleconferencing Consortium (IMTC) VoIP Forum.
- **ITU G.729A:** This algorithm runs at 8 Kbps with a 35 ms total system delay. It provides near toll-quality performance and is ideal for applications requiring high-quality speech coding with low delay. G.729A has been deployed for many years as the speech encoder of choice for the Frame Relay market. G.729A is the alternate default encoder for IP telephony chosen by the IMTC - VoIP.

Table 3.2-5 presents the MOS score for a set of popular coding algorithms. As previously explained, the MOS is an opinion rating method that is used to assess the degree of quality for a speech processing system. In this method, listeners rate the speech under test on a five-point scale where a listener's subjective impressions are assigned a numerical value. The rating scale for the MOS is presented in Table 3.2-6.

Table 3.2-5: Coding Standards and Corresponding MOS

Coding Standard	Compression Algorithm	Bit Rate (kb/s)	MOS Score
G.711	PCM	64	4.4
G.726	ADPCM	32	4.2
G.728	LD-CELP	16	4.2
G.729	CS-ACELP	8	4.2
G.729A	CS-ACELP	8	4.2
G.723.1	MP-MLQ	6.3	3.98
G.723.1	ACLEP	5.3	3.5

Table 3.2-6: Mean Opinion Score Five-Point Scale

Rating	Speech Quality	Level of Distortion
5	Excellent	Imperceptible
4	Good	Just perceptible but not annoying
3	Fair	Perceptible and slightly annoying
2	Poor	Annoying but not objectionable
1	Unsatisfactory	Very annoying and objectionable

3.2.3 Comparison

The preceding discussion has shown that a managed IP network can easily provide toll quality voice services that meet FAA requirements for latency. The FAA requirements for availability can be more rigorously defined with a packet network, which, if properly engineered, will meet these requirements as well. A summary of the recommendations in this section for voice over packet services includes:

- Dropped Packets – network should be required to perform at better than 10% lost packet rate.
- Latency – this imposes several network constraints, including:
 - Use of header compression
 - Use of traffic shaping
 - Limiting path length to five router hops
- Echo – Echo cancellation equipment supplying 40 to 50 dB of echo cancellation is optimal.
- Jitter – Jitter buffering is required, but its use should be balanced against increased latency.
- Vocoder Selection – the ITU-T G.729A vocoder is recommended for this application.

3.3 SECURITY

3.3.1 FAA Information Security Requirements

In recent years FAA has faced new information systems security (ISS) requirements mandated by the Computer Security Act of 1987; the Office of Management and Budget (OMB) Circular A-130, *Management of Federal Information Resources*; the Department of Transportation (DOT) Handbook, DOT H 1350.2, *Departmental Information Resources Management Manual* (DIRMM); and Presidential Directive (PDD) 63²⁹. These have resulted in several FAA security initiatives leading to the development of new ISS policy and requirements documents. Foremost of these new documents is FAA Order 1370.82, *Information Systems Security Program*³⁰, which establishes FAA high-level ISS policy and assigns organizational and management responsibilities to ensure implementation of the aforementioned Federal statutory, policy, and regulatory mandates. Order 1370.82 cancels earlier FAA Orders related to system security (1600.54B and 1600.66) and has precedence over other FAA Orders that contain conflicting, incomplete, or obsolete ISS policy.

Another key FAA security document applicable to the activities of this study is the *Information System Security Architecture*³¹, which provides a top-level design for integrating security into the NAS. This document provides ISS architecture design guidance that has been utilized a great deal for this study.

A third applicable FAA document is FAA Order 1830.9, *Wide Area Network Security*³² (still in draft form), which establishes and defines security policy and procedures that apply to the implementation, connection, and use of FAA WANs.

Requirements specified in these three documents that are applicable to this study, that is, those that guide the selection of security technologies for the future NAS communications architecture, are presented in the following sections. It must be stressed that FAA security policy and requirements are works in progress, and should continue to evolve. For that reason, security requirements used for this study, for the most part, represent high level FAA requirements, rather than specific, detailed requirements, as the high-level requirements are less likely to change significantly over time, and are most useful for providing general guidance in defining NAS communications architectures.

3.3.1.1 Applicable Information Systems Security Program Requirements

Though Order 1370.82 mostly specifies responsibilities of FAA organizations in the implementation of ISS programs, it includes several high-level ISS policies and requirements that apply to the implementation and maintenance of all NAS systems. These include the following:

- The new baseline security level for information systems is derived from Commercial Off The Shelf (COTS) Security Protection Profiles (CSPP) published by the National Institute of Standards and Technology (NIST), the National Security Agency (NSA), or under Common Criteria Mutual Recognition Arrangements (MRA) with either agency. (The previous baseline security level was based on Department of Defense security criteria).

- 1370.82 requires ISS compliance reviews and site surveys not only for those information systems located in FAA facilities, but for all FAA information systems, including FAA information systems developed, operated, or housed in non-FAA facilities, as well as for equipment not owned by the FAA, but operated on behalf of the FAA.
- Security is to be implemented at a level commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to, or modification of, FAA information.

3.3.1.2 Applicable Information System Security Architecture Requirements

3.3.1.2.1 Introduction

As described in *Information System Security Architecture*, proposed ISS Architecture security services are ISS requirements allocated to NAS subsystems that process, communicate, and control sensitive ATC information. These subsystems are mapped into three functional categories: 1) computer platform, 2) communications, and 3) management/administration. Of these, communications requirements are most relevant to this study.

Generally, the ISS Architecture communications requirements call for security services to be implemented with COTS products. In addition, the Communications Security Strategy presented in the *Information System Security Architecture* provides a three-tier hierarchy of physical and logical networks to control access based on levels of trust:

- Networks for NAS operation (intranet)
- NAS partners and suppliers (extranets)
- Public interchange (Internet)

The Communications Security Strategy also provides concepts useful for FAA infrastructure protection, including the Common Network Security Interface (CNSI) and the Common Network Security Model (CNSM). The CNSI is a firewall-based VPN for communicating between FAA LANs and public WANS. The CNSM provides a configuration for routing, authenticating, and compartmenting user communications at multiple trust levels concurrently. These two concepts are discussed in more detail in later sections of this report.

It should be noted that the *Information System Security Architecture* recognizes that telecommunications systems, such as the proposed FTI, cannot provide all the security services required for CSPP-level protection of end-user information. End-user systems are ultimately responsible for providing security features that ensure the protection of sensitive data as well as preventing the compromise of the network through use of systems. The FTI approach is to employ a set of end-user connections and service delivery point (SDP) criteria to maintain minimum standards among all connected systems to help mitigate the risk of compromise to the network to an acceptable level.

It also should be noted that the *Information System Security Architecture* document recognizes the issue of the FAA's commitment (at least for international ATC) to Aeronautical Telecommunications Network (ATN) requirements, which are based on International Standards Organization (ISO) protocols, and the general lack of ISO standards-based COTS products or commercial services in this country. ISO standards-based COTS security products are so scarce primarily because of the adoption of TCP/IP as the de facto standard protocol for modern data communications networks. It is assumed that the FAA will find an effective and harmonious resolution of this issue, such as approaches that encapsulate ATN data over IP; and therefore application of IP-based protocols and COTS products will be the focus of this study.

3.3.1.2.2 Specific Guidance Provided by the *Information System Security Architecture*

The *Information System Security Architecture* requirements (excluding physical and personnel security requirements) for communications and infrastructure consist of the following:

- (C1) The system shall be capable of transmitting and receiving cryptographically processed data at the transport layer and below.
- (C2) The system shall implement strong authentication of network users.
- (C3) The system shall implement screening/firewall/proxy server functionality, as appropriate.
- (C4) The system shall be the object of periodic network-based vulnerability assessments.
- (C5) The system shall maintain and protect comprehensive logs of Security Relevant Events from unauthorized destruction or modification.
- (C6) The system shall be capable of detecting and removing malicious code and data from communications data.
- (C7) The system shall implement network-based intrusion detection.
- (C8) The system shall protect information system security data and functionality from all unauthorized access.

These requirements, with the exception of C4 and C5, which are more operational related, formed the guidance for the selection of the security architecture defined for this study.

3.3.1.2.3 The Common Network Security Interface ³³

To meet the ISS architecture security requirements specified above and to support the development of the NAS-Wide Information Network (NASWIN) proposed in the NAS Architecture 4.0, the ISS architecture has developed the concept of a Common Network Security Interface for each NAS subsystem. The basis of the CNSI, envisioned for the 2005 – 2008 timeframe, is the implementation of a series of Operations Data VPNs to provide security for the NASWIN in support of the NAS subsystems. The CNSI concept may either be implemented as a bastion host or as security software resident on an already-available front-end machine. The CNSI security functionality may be divided among a number of devices managing a facility's WAN interface. All forward and return information and data exchanged by NAS facilities with

external users transits its local CNSI (see Figure 3.3-1). Each deployed CNSI provides the following network security services:

- VPN support for its facility's subsystems exchanging sensitive data across untrusted WAN segments. Data encryption is required as part of this VPN functionality.
- Network access control mechanisms that permit or deny external processes access to facility subsystems based on authenticated device and process identification and controlled access protection logic.
- Data confidentiality services that control the transmission of certain classes of sensitive data.
- Strong authentication capabilities for external individuals, devices, and processes requesting services.
- Virus detection and removal.
- Self-protection of its own platform environment through the use of ISS architecture platform security requirements.

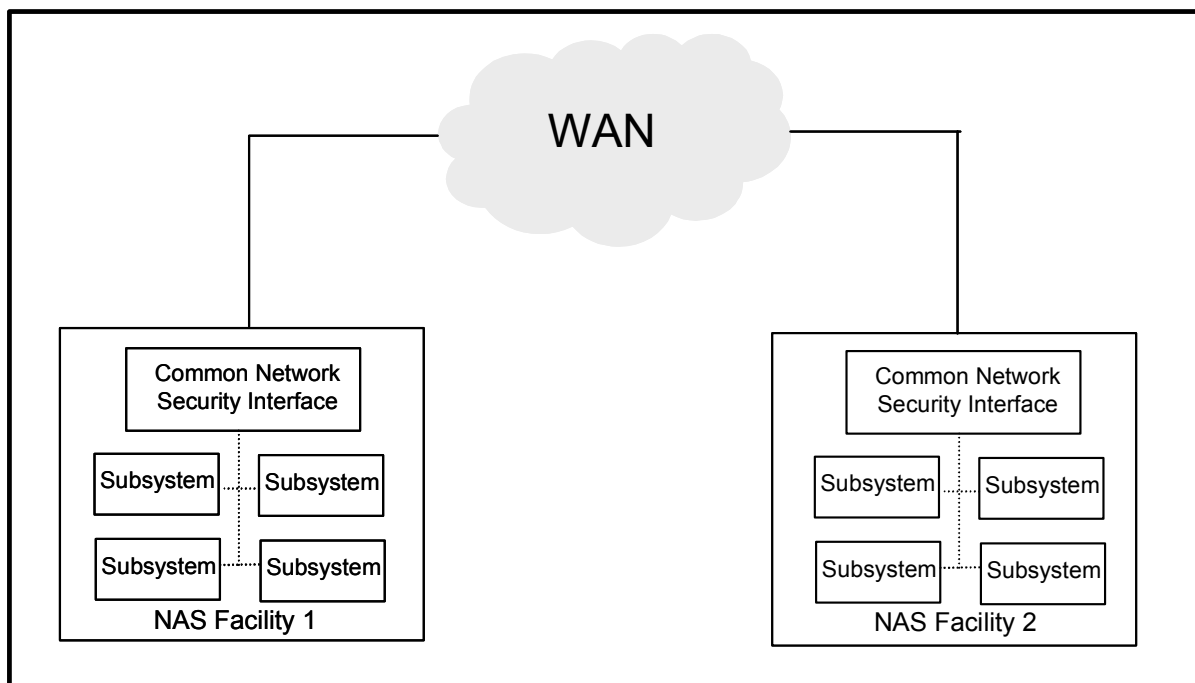


Figure 3.3-1: Common Network Security Interface

3.3.1.2.3.1 Recommended CNSI Implementation ³⁴

The *Information System Security Architecture* has recommended an implementation approach for the CNSI. This approach has been adopted for the definition of NAS communications architecture for this study. The approach consists of the following:

- Start with a VPN that uses encryption to tunnel communications through less trusted networks.

- Use a firewall-based VPN; the firewall controls access to local networks (LANs) by checking router addresses of external users.
- Choose a stateful-inspection firewall to optimize performance by operating the firewall and VPN at the same layer of the OSI Reference Model (RM). (Stateful-inspection uses connection history for precise access control).
- When the external network has multiple hosts, use a screened subnet firewall (see Section 2.2.5.2.3 for a description of a screened subnet firewall) for routing external communications and concealing addresses on the intranet.
- A screened subnet firewall routes traffic to and from the DMZ network. A bastion host with a secure operating system is needed to protect traffic while in the DMZ network.

Traffic flow through the recommended firewall based VPN is described and depicted in Figure 3.3-2.

Incoming VPN Traffic

- Incoming VPN packets are directed to the VPN device. The VPN device strips off the encryption overhead on the packet and checks for authentication privileges, such as user authentication.
- The packet is then routed to the firewall for IP address verification. As an additional safeguard, network address translation (NAT) is performed by the firewall. NAT readdresses the packet to its original (internal) IP address thereby preventing external access to the LAN.
- The firewall/NAT device then routes the packet (with its internal IP address) to the internal router.

Outgoing VPN Traffic

- All traffic coming from the internal router is directed to the firewall/NAT device to change the source IP address of the requesting device to a routable public IP address.
- The firewall/NAT device then forwards the packet to the VPN device that performs the encryption process for that packet. The packet is routed to the external router and finally to its destination.

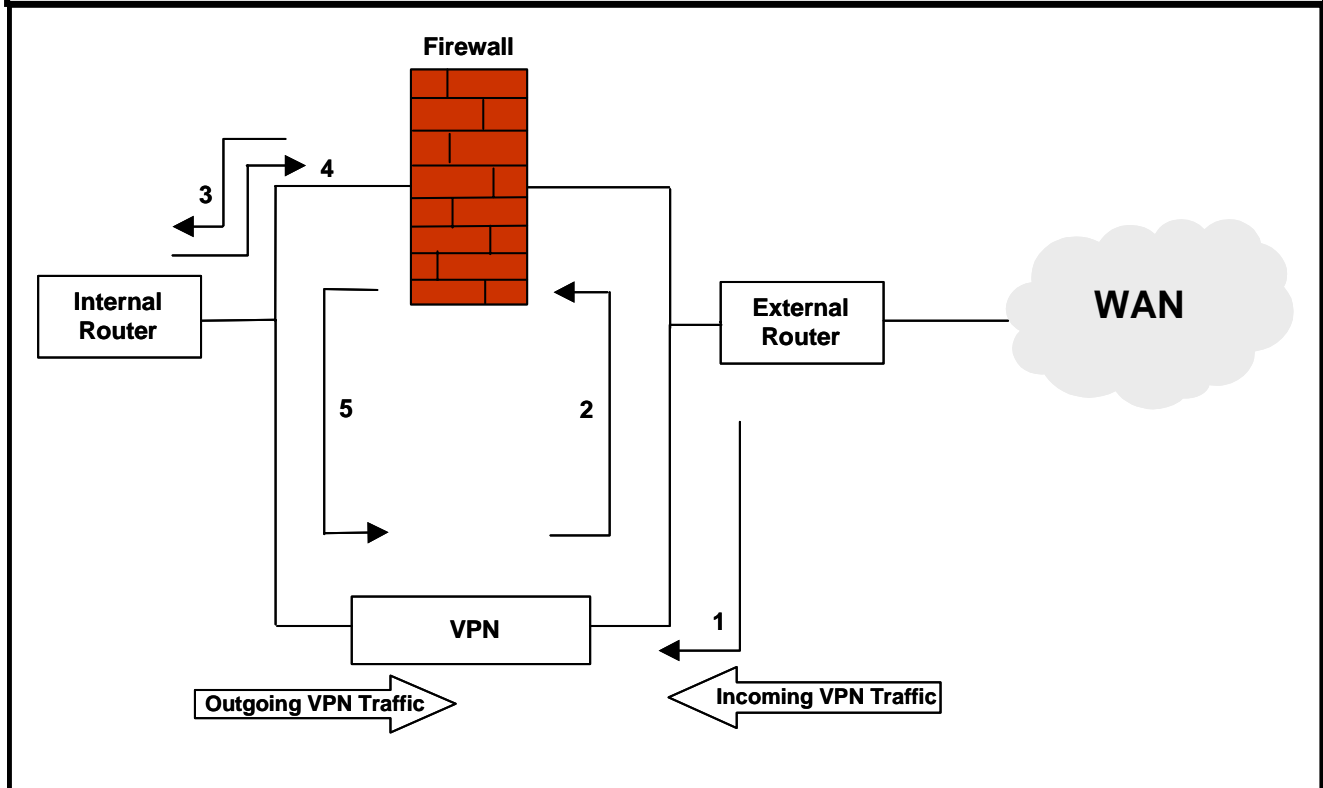


Figure 3.3-2: Firewall Based VPN

3.3.1.2.4 The Common Network Security Model³⁵

The CNSM provides guidance on how the CNSI can provide layered access control to FAA, privileged (extranet), and public (Internet) users according to levels of trust. The CNSM, shown in Figure 3.3-3, consists of a firewall and a VPN implemented with a bastion host in a screened subnetwork configuration. In this configuration, the bastion host is separately connected to LANs in the DMZ, an internal router to the facility LAN, and an external router to WANs. Extranet and Internet proxy servers are access points for exchanging information between intranet hosts in the facility and external users. The CNSM operates as follows (with outgoing messages following the reverse path of the incoming messages):

- The bastion host implements both the VPN and firewall in hardware or software. It uses a secure operating system to protect itself and integrity of communications with routers and DMZ LANs.
- The firewall provides NAT for all messages.
- FAA (intranet) users communicate with VPNs over public WANs. Intranet messages are routed using IP addresses through the external router, VPN, firewall, and internal router to the facility LAN.
- Privileged (extranet) users communicate with VPNs over public WANs. Extranet messages are routed using IP addresses through the external router, VPN, firewall, and DMZ LAN to an extranet server.
- Public (Internet) users communicate over public WANs. Messages are routed using IP addresses through the external router, firewall, and DMZ LAN to an Internet proxy server.
- FAA users on the local facility intranet LAN communicate with extranet and Internet proxy servers through the internal router, firewall, and DMZ LANs to access and upgrade information. Messages are routed using internal IP addresses that are recognized by the firewall and shielded from external users by NAT.
- The FAA intranet is comprised of all automation system LANs and only authorized FAA personnel and systems may exchange data through inter-facility WANs. All messages between trusted facilities will utilize VPNs.
- Data may be transmitted without a firewall or VPN where a remote trusted subsystem connects with a trusted (FAA owned) communications system to the local facility.

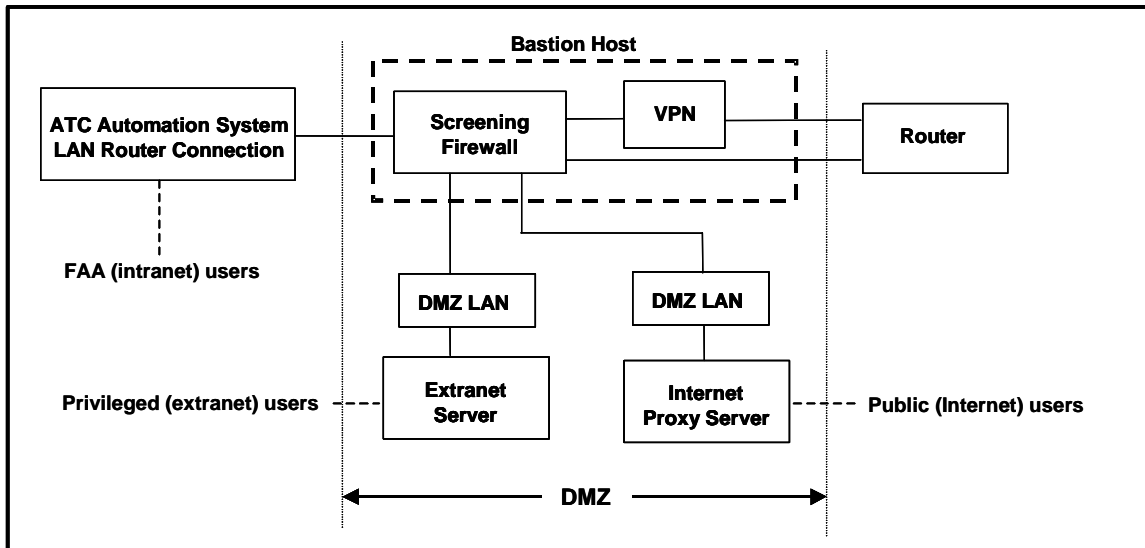


Figure 3.3-3: Common Network Security Model

Table 3.3-1 summarizes CNSM operations.

Table 3.3-1: CNSM Operation Summary

Level of Trust	Protocol	Firewall	VPN	Server
FAA (intranet) user	ATN/IP or TCP/IP	X	X	
Privileged (extranet) user	ATN/IP or TCP/IP	X	X	Extranet
Public (Internet) user	TCP/IP	X		Internet proxy

The NAS communications architecture definition developed for this study followed the CNSM, except that connections to the Internet were not considered.

3.3.1.2.5 Cryptographic Processing and Key Management

3.3.1.2.5.1 Cryptographic Processing

The *Information System Security Architecture* recommends the implementation of IPSec to provide network layer NAS ISS. As mentioned above, the upper ATN layers of the NAS can be transmitted over an IP subnetwork through encapsulation. Security can be extended to the NAS application layer processes or NAS end users by additional security (not IPSec) provided at the application layer. IPSec, as described in Section 2.2.3, offers a host of cryptographic features suitable for FAA, with the Tunnel Mode offering the most flexibility with NAS subsystems and applications. The FAA favors symmetric cryptographic processing standards – those that utilize secret keys, rather than public key (asymmetric) standards, because secret-key based cryptographic processing is normally much faster, more secure, and involves smaller key sizes for comparable security. However, because COTS security products usually

provide a hybrid (symmetric/asymmetric mixture) approach, it is expected that the NAS ISS architecture will make some use of these. The Secure Socket Layer (SSL) v.3 protocol is a commonly used example of such a hybrid approach.

The determination of a NAS ISS recommended symmetric encryption standard has not yet been made, but the recently chosen Advanced Encryption Standard (AES) has been identified as a good candidate.

3.3.1.2.5.2 Key Management - Public Key Infrastructure ³⁶

The NAS Public Key Infrastructure (PKI) is the entire organizational, technological, and procedural elements that allow for the widespread use of both asymmetric and symmetric cryptographic processes. It does this by establishing an infrastructure through which NAS-wide public-key cryptographic material is made available to all users within the NAS. A suitable PKI must contain the following elements:

- Certification Authorities (CAs) that issue and revoke certificates.
- Organizational Registration Authorities (ORAs) that vouch for the binding between public keys and certificate holder identities and other attributes.
- Certificate holders that are issued certificates and can sign digital documents.
- Clients that validate digital signatures and their certification paths from a known public key of a trusted CA.
- Repositories that store and make available certificates and Certificate Revocation Lists (CRLs).

A PKI enables an enterprise wide certification and publication of public-key material, which in turn enables most other enterprise wide cryptographic services.

Because PKI relevant standards are still under development, ISS recommended approaches can not yet be made. However, a tentative ISS PKI strategy is as follows:

- Implement top level CAs (one primary and one backup) within an X.500/X.509 based PKI.
- Establish a limited number of IP based gateways at designated ATC facilities.
- Establish necessary client-server relationships between CAs and designated ATC facilities to facilitate PKI, i.e., X.500 directories, Certificate Servers, Digital Signature Algorithms (DSAs), Directory User Agents (DUAs), etc.
- Establish the IP based gateways as participants in the NAS PKI, having the CAs issue certificates for them.
- Implement PKI enabling functions within the VPN gateways to allow them to obtain and exchange necessary key material among themselves.
- Extend PKI to other designated IP based functionality within the NAS.
- Extend the PKI to the ATN domain.
- Extend NAS ISS services to the ATN domain

- Extend security services to other IP and non-IP based communications domains, using the NAS PKI and necessary gateway functionality.

3.3.1.3 Applicable Wide Area Network Security Requirements

Although the draft version of this document available for this study is fairly recent, it is at least partially based on some earlier FAA security documents (Orders 1600.54B and 1600.66) and may not be in complete harmony with the other two, more recent documents just discussed. Nevertheless, it does offer some utility for this study, as it provides some general requirements relating to the provision of firewalls and routers for FAA LAN/WAN infrastructure that are compatible with the higher-level requirements presented in the other two documents. These include the following:

- LANs with direct external connections, such as dial-up access or Internet access, shall install and maintain a security access device (e.g., firewall, router, gateway, Remote Access Service (RAS), etc.) that controls and limits external access to FAA information systems.
- FAA perimeter access control devices shall be configured to deny all services not expressly permitted.
- FAA firewalls shall provide an intrusion detection capability to detect unusual security events and provide an alert when this happens.
- FAA firewalls shall provide NAT to obscure FAA WAN and organizational LANs internal IP addresses from the Internet.
- FAA firewalls shall support VPN technology and meet the following VPN requirements:
 - The VPN shall be used to ensure the privacy and integrity of data as it traverses the external non-trusted Internet.
 - FAA systems that communicate using custom application protocols over the Internet shall use VPN technology to authenticate and encrypt the communications.
 - The VPN shall provide a means, such as public/private keys, digital certificates, or other strong authentication mechanism, to verify the identity of systems and remote users.
 - The VPN shall ensure that data carried on the public network is unreadable to unauthorized clients through the use of at least 56-bit or higher DES encryption technology.

3.3.2 Applying Security Technologies to FAA Security Requirements

Earlier portions of Section 3 have compared the FAA's needs for data, voice, and video services to available network communications services to assess how well these services would fulfill FAA requirements. In many cases, the FAA's needs and requirements are based on legacy systems and/or functionalities with fairly definitive requirements, and thus provide sufficient guidance to evaluate the available services. However, security requirements present a different case. It has been found that, without a significant legacy of security systems and services, the FAA's nascent communications security needs and requirements are being shaped a great deal by current standards-based technologies and

systems, mostly spurred by the emergence of IP based networks as the predominant standard for worldwide data communications. Therefore, not only are COTS products available to satisfy the FAA's security requirements, COTS products are mandated. Even the FAA's need to comply with ATN standards can be accommodated through a combination of application level security products and encapsulation of the ATN upper layer protocol information in IP packets.

3.4 ENTERPRISE MANAGEMENT

3.4.1 Introduction

Enterprise Management, in the context of an FAA NAS communications architecture based on leased network services, involves both the service providers and the FAA. Both the service providers and the FAA have to implement their own enterprise management strategies, but must be able to exchange Network Management information and accommodate the other elements of their respective Enterprise Management systems. This can be accomplished through the adoption, by both parties, of standards-based services and systems to provide compatibility across their mutual interface. Figure 3.4-1 presents an FAA architecture concept, showing enterprise management elements for both the FAA and the telecommunications service provider. This figure implies a general FAA need for enterprise management without specifying particular implementations or requirements.

This section presents an assessment of FAA needs for the following specific aspects of enterprise management:

- Network Monitoring and Management
- Management of IP address space
- Time distribution services
- Network directory services

Following the FAA needs assessment for each of the enterprise management elements is a discussion of how the enterprise management technologies and services described in Section 2.4 could be applied to the identified needs.

3.4.2 Network Monitoring and Management

The current FAA telecommunications infrastructure is predominately a leased-private-line, dedicated network, in which performance management is straightforward. Essentially, network status is a simple matter of a circuit being operational or not. As the FAA migrates towards leasing packet network communications services, the service provider should provide network management of assets supporting the leased communications service. The service provider also should provide FAA designated systems with standards-based real-time and historical management information on the leased system. The FAA Network Manager will integrate the management data from the telecommunications service provider,

legacy telecommunications systems, and end user systems to provide end-to-end service management (See Figure 3.4-1).

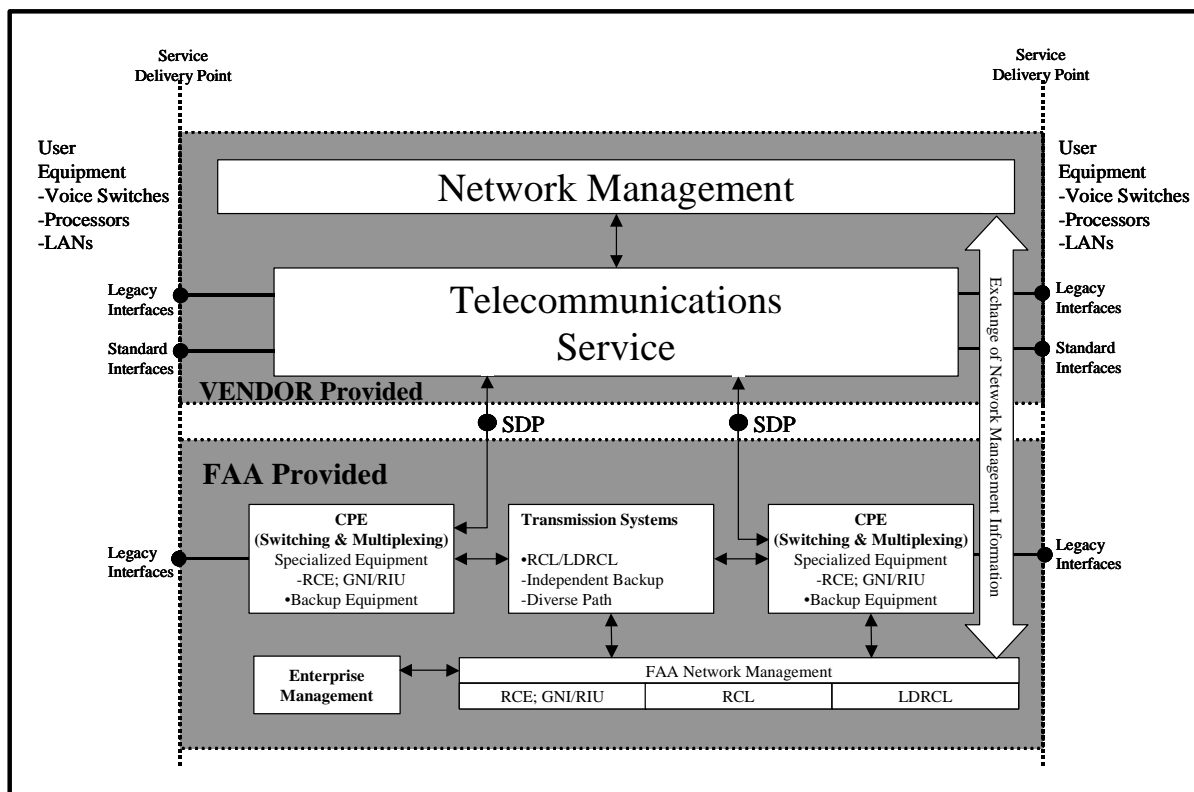


Figure 3.4-1: Telecommunications Architecture, Showing Enterprise Management Elements

One way to implement this integration would be for the FAA to specify a TIMS database interface where the service provider collected data would reside. In this concept the collection of network data would be a service provider responsibility, while analysis of network data would be an FAA responsibility.

3.4.3 Management of NAS IP Address Space

Recall from Section 3.2.4.3, that management of an IP address space includes:

- Allocation of IP addresses to facilities/programs.
- Assignment of IP addresses to hosts.
- Adoption of a naming convention that maps names (based on a hierarchical naming structure) to IP addresses.
- Implementation of the DNS: location and number of Domain Name Servers.

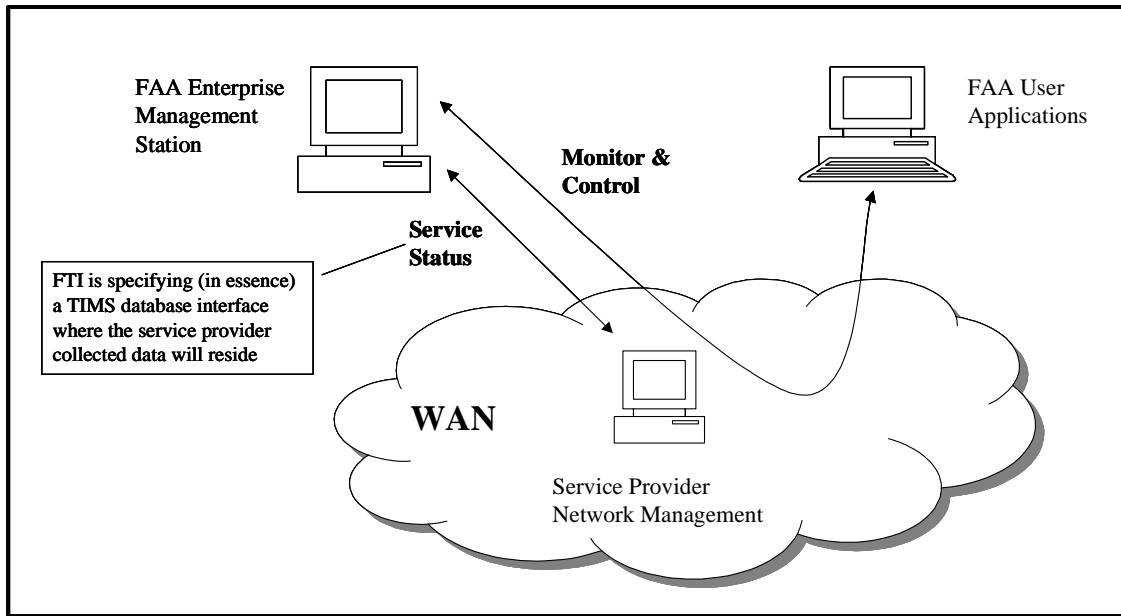


Figure 3.4-2: FTI Concept of Collection of Network Management Information

3.4.3.1 FAA Allocation of IP Addresses to Facilities/Programs and Hosts

Table 3.4-1 describes the private IP address assignments that are valid on all FAA LANs and WANs as described in document ENET 1370-002.7, FAA Enterprise Network Internet Protocol Version 4 (Ipv4) Non-NAS Internet/Intranet Address Assignments, November, 2000. The FAA is implementing this private IP addressing plan to provide virtually unlimited IP address space (IPV4), while providing a level of security (enhanced with firewalls) that should provide agency data telecommunications assets with the level of protection they require. As part of this IP addressing plan, the FAA stopped utilizing most public IP addresses in January 1998. This was accomplished in a two-step approach that began in October 1997.

Table 3.4-1: Private IP Assignments Summary^{37 38}

Private IP Assignments³⁹	Who assigns—	Where it is valid—
10.x.x.x Assignments		
<i>10.0.x.x (Class A)</i>	<i>ENOCC</i>	<i>Reserved</i>
10.1.x.x – 10.150.x.x	Multiple <i>Initial Regional address block assignments are made by the ENOCC (Enterprise Network Operations Control Center). The ETCs and local LAN Administrators make address assignments within the allocated block(s). ARTCC address assignments are made by the ENOCC (in consultation with the Regional ETCs and ATS representatives).</i>	FAA-Wide
10.151.x.x – 10.254.x.x	ENOCC	NAS/ATC ⁴⁰
<i>10.255.x.x</i>	<i>ENOCC</i>	<i>Reserved</i>
172.x.x.x Assignments⁴¹		
172.16.x.x – 172.28.x.x (Class B)	Region ETC <i>Private 172.x Class B addresses are assigned by the Region ETC for use by any network device directly connected to the Regional backbone.</i>	Primary Region HQ
172.29.x.x	<i>ENOCC</i>	<i>Reserved</i>
172.30.x.x	<i>ENOCC</i>	<i>Reserved</i>
172.31.x.x	ENOCC	NAS/ATC
192.168.x.x Assignments		
192.168.0.x – 192.168.110.x (Class C)	ENOCC	NAS/ATC
<i>192.168.111.x – 192.168.220.x</i>	<i>ENOCC</i>	<i>Reserved</i>
192.168.221.x – 192.168.254.x	Multiple	Internet Access Sites (AWA, AMC, and AWP)
<i>192.168.255.x</i>	<i>ENOCC</i>	<i>Reserved</i>
239.x.x.x.		
239.x.x.x (Class D)	ENOCC	FAA-Wide

3.4.3.1.1 Operational IPv4 Address Assignments

Table 3.4-2 summarizes the IPv4 address allocation defined for the purposes of Air Traffic Control (ATC) and Air Traffic Management (ATM) within a NAS intranet.⁴²

Table 3.4-2: Summary of Operational IPv4 Address Allocation

FACILITY TYPE	IPv4 ADDRESS RANGE
Reserved	10.150.0.x to 10.151.255.x
ARTCCs	10.152.0.x to 10.154.223.x
Reserved	10.154.224.x to 10.155.191.x
FAA Academy	10.155.192.x to 10.156.63.x
WJHTC	10.156.64.x to 10.156.191.x
ATCSCC	
Reserved	10.156.192.x
Central Flow	10.156.193.x to 10.156.202.x
Reserved	10.156.203.x to 10.156.212.x
NOCC	10.156.213.x to 10.156.222.x
Reserved	10.156.223.x
ETMS Hubs	10.156.224.x to 10.156.255.x
TRACONs	10.157.0.x to 10.178.159.x
Reserved	10.178.160.x to 10.184.127.x
WAAS	10.184.128.x to 10.184.159.x
OCCs	10.184.160.x to 10.184.255.x
ATCTs (not collocated with TRACONs, does not include DoD towers, except Scott AFB)	10.185.0.x to 10.226.191.x
Reserved	10.226.192.x to 10.234.255.x
FSSs	10.235.0.x to 10.245.255.x
Reserved	10.246.0.x
Alaska NAS Interfacility Communications System (ANICS)	10.246.1.x to 10.246.249.x
Reserved	10.246.250.x to 10.246.255.x
Reserved for DoD STARS	10.247.0.x to 10.248.255.x
Reserved	10.249.0.x to 10.255.252.x
NIMS Development	10.255.253.x to 10.255.254.x
Reserved	10.255.255.x
Reserved	192.168.0.x to 192.168.9.x
NIMS-ALERT	192.168.10.x to 192.168.18.x
Reserved	192.168.19.x to 192.168.110.x

3.4.3.2 Adoption of a Naming Convention that Maps Names to IP Addresses

In a supplement to the Enterprise Network Program (ENET)⁴³ ENET1370-005.3, the FAA has already defined the method by which names are to be selected for domains, and has defined the criteria to be followed when setting up name servers on the network. As part of this supplement, the FAA has defined the topology for NAS internet/intranet access and the associated DNS structure. The current FAA Name Space Domain Structure is shown in Figure 3.4-3.

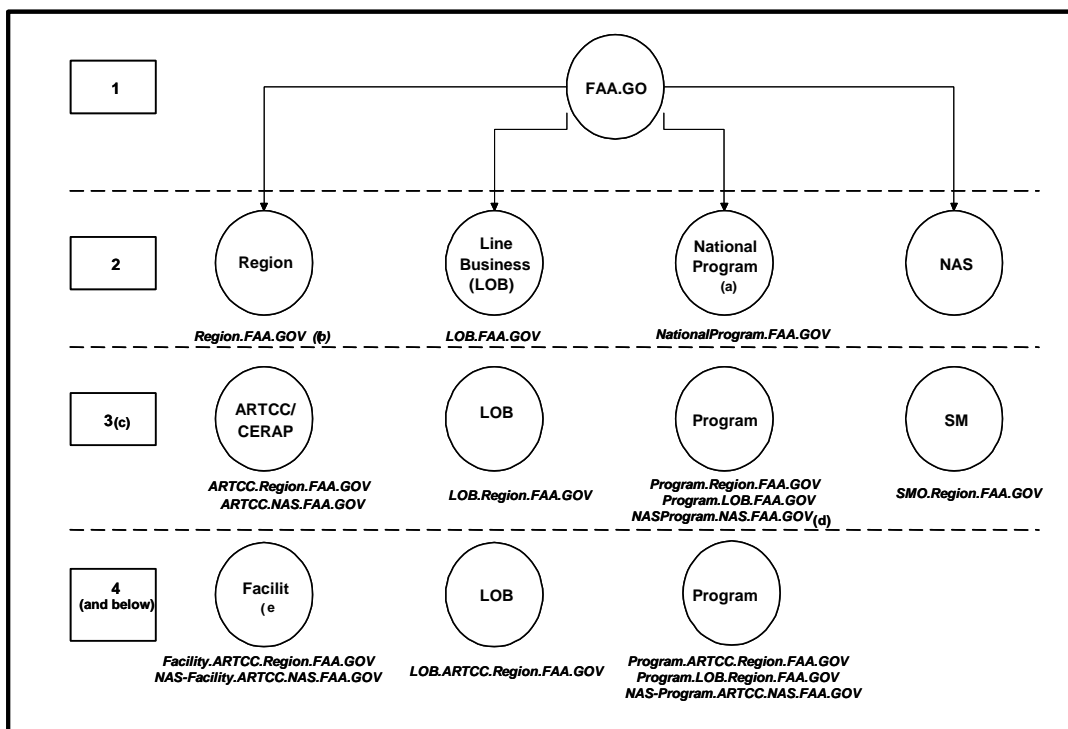


Figure 3.4-3: FAA Name Space Domain Structure

3.4.3.3 Implementation of the Domain Name System (DNS): Location and Number of Domain Name Servers

The guidelines for this implementation are defined in ENET1370-005.1B⁴⁴. This document describes procedures for implementation of security measures, including screening routers, screened subnet (DMZ), proxy servers, firewalls, and a private IP plan. Three FAA sites are selected as FAA-wide Internet access points: AWA in Washington DC, AMC in Oklahoma City, OK and AWP located in Los Angeles CA. ACT will also have an Internet access point that will serve only ACT.

ENET 1370 provides for separate DNS servers for public and private IP addresses for security reasons. It specifies the use of both private and public DNS servers at each of the three Internet access sites. Each site should have one primary private server and two secondary servers (same for public). Private and public DNS architecture supports a root level domain structure that utilizes the name space of FAA.GOV. Orgs/programs/LOBs will have the option to maintain a private DNS server for a sub domain under FAA.GOV. Figure 3.4-4 illustrates this architecture.

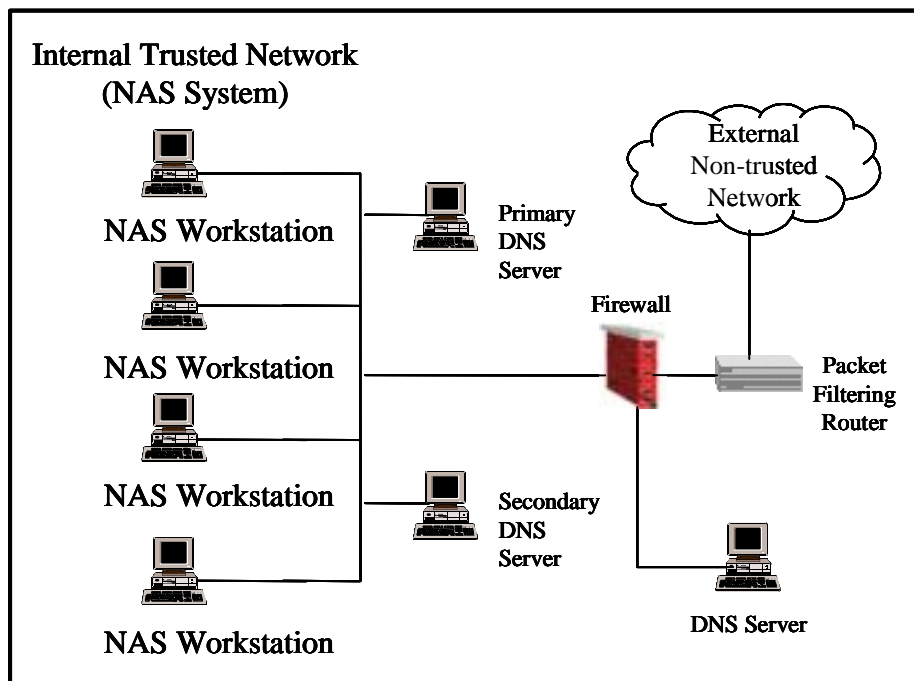


Figure 3.4-4: Location and Number of DNS Servers

3.4.4 Network Time Distribution

3.4.4.1 Time Distribution Service Requirements in the NAS

There are several reasons why accurate and stable timing is needed for NAS communications:

- **Proper operation.** Certain NAS systems, such as surveillance systems and the anticipated VHF Digital Link (VDL) Mode 3 implementation of the Next Generation Communication System (NEXCOM), are heavily reliant on accurate and stable timing for proper operation. Primary surveillance system tracking accuracy depends on accurate time comparison between transmitted and received pulses, while the NEXCOM VDL Mode 3 Time Division Multiple Access (TDMA) system requires stable and accurate timing to transmit and receive via assigned channel time slots.
- **Network fault isolation, reporting, and restoral.** Having precise time indication of NAS infrastructure faults and failures would aid in the accurate reporting of these events and would be necessary to track their duration and ultimate restoral.
- **Network monitoring, measurement and control:** This goes beyond time indication of faults/failures and includes the need to continuously track the performance and status of NAS infrastructure and provide time critical control signals to the infrastructure. Certain communications performance measurements, such as bit error rate, can only be performed with accurate and stable timing.
- **Precise and accurate time stamps on user data.** There are certain types of data in the NAS, e.g. surveillance data, that require precise and accurate time stamps in order to properly track aircraft and provide this information to NAS automation systems and ultimately to the controller.
- **Security.** There are several needs for accurate time indication to provide adequate NAS security. These include the need for time stamps on computer logs to accurately track network access, and the need for accurate time indication during authentication processes.
- **File synchronization.** In a networked automation system with file sharing, accurate time is necessary to keep files synchronized and thus ensure use of the latest data and/or required file version.

3.4.4.2 Application of Time Distribution Technologies to the NAS

As discussed in Section 2.4.4, there are numerous methods to implement timing distribution for a network, depending on the network's timing requirements, sensitivity to cost, and the accessibility to the various sources of accurate timing. It has been found that timing synchronization performance of networks/systems increases with the proximity of the nearest PRS. Providing network synchronization for NAS communications could be achieved through a combination of methods, depending on the application and the time criticality of the application. For the most part, timing distribution over NAS WANs using NTP would be sufficient and cost effective for non-critical NAS services. For these cases network service providers would provide timing via PRSs at their facilities. This would provide WAN synchronization accuracy in the tens of milliseconds range. As NAS communications evolve towards IP networks, this would have a minimal cost impact to load (no-cost or low-cost) NTP software on each NAS network client/server.

Other NAS systems with more stringent timing requirements (e.g., NEXCOM, surveillance systems, etc.) would require on site Network Time Servers with PRS input, typically GPS. These would provide at least < 1 microsecond timing accuracy (typically much better than this, in the sub-parts per million range) through direct connection with the PRS, and synchronization accuracy for networked components on site in the 1 millisecond to 1 microsecond range. This would have more than a minimal cost impact, as Network Time Servers can cost several thousand dollars apiece.

3.4.5 Network Directory Services - NAS Common Directory Service

As stated in Section 2.4.5, for distributed systems there exists a need for standards-based common directory services. Thus, Directory Services is an important function that should be implemented in the NAS network architecture, especially for the following important reasons:

- It is most cost effective to maintain and use.
- It avoids “balkanization” problems of implementing numerous “hard-wired” directories for each NAS system.
- It is scalable.
- It facilitates sharing of data.
- It provides a uniform approach to data warehousing.
- It provides a common data standard.

4. APPLICATION OF AVAILABLE SERVICES/TECHNOLOGIES TO ZOB

4.1 OVERALL ARCHITECTURE DESCRIPTION

An objective of the Task-11 study is to explore the synthesis of FAA facility communication requirements and COTS network components. To achieve this goal, an understanding of FAA communication architecture and requirements as well as commercial network backbone architecture and services was required. This section outlines the methodology and results of the process used to describe commercial backbone network architectures and services; identify a subset of FAA sites to analyze; determine communication requirements of the FAA sites; and specify the connection to, and use of commercial networks to satisfy FAA communication requirements. During the course of the work, optimization criteria were used to define an architecture that minimizes cost and complexity while meeting capacity, latency and availability constraints.

The overall architecture vision is to provide a standard set of network services and interfaces. This architecture is assumed to embody the vision of the NAS Integrated Network including standard network services, network layer security, enterprise management services, and support of legacy networks and/or provision of legacy interfaces (via gateways). A depiction of the overall architecture vision is provided in Figure 4.1-1 below.

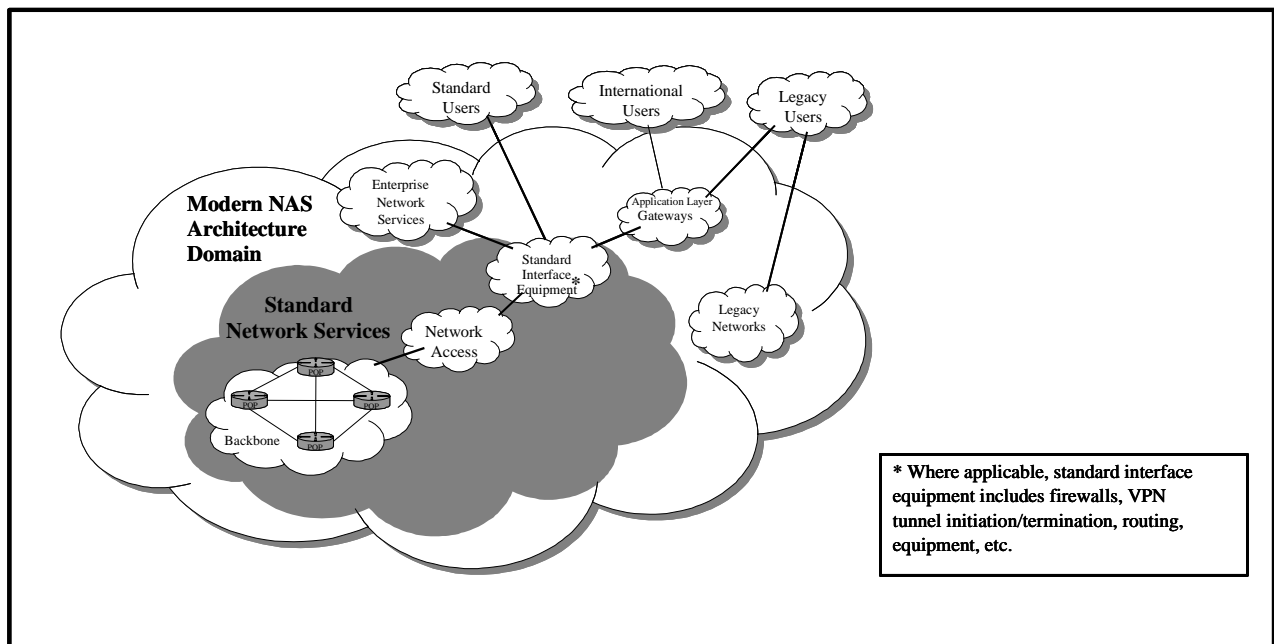


Figure 4.1-1: Overall NAS Architecture Vision

To analyze the implications of such an architecture vision, including performance, cost, and transition, a portion of the Cleveland ARTCC (ZOB) area was selected as a representative site in which to study the

application of the NAS architecture vision. The specific process and results for defining the ZOB area architecture are described in detail in the following subsections. They include:

- 4.2 Description of Commercial Managed Backbone Networks
- 4.3 ZOB Facilities Selected for Analysis
- 4.4 ZOB Nodes Definition and Communication Requirements
- 4.5 Connecting Nodes to Backbone Networks
- 4.7 Network Equipment at FAA Nodes and Network Circuits

4.2 DESCRIPTION OF COMMERCIAL MANAGED BACKBONE NETWORKS

In this report, Section 3.1 provides an overview of the current state of commercial dedicated backbone networks⁴⁵ and services. This section examines this material in light of FAA communication requirements; considers backbone network architecture trends; and outlines backbone architecture scenarios for consideration in this study.

4.2.1 General Architecture and Performance

The migration of the NAS from a point-to-point architecture to a network architecture utilizing modern technology has been the subject of several documents and studies in the past few years.^{46,47,48} In these documents, focus is on specifying a FAA-specific network topology and technology. A more recent study⁴⁹ examined trends in network architectures and services and determined whether a FAA network should be specified in terms of topology and technology, or whether this detail should be transparent to the user (i.e. cloud topology utilizing commercial backbone networks). The Task 10 study results indicated that several benefits result in this latter approach, including:

- An approach not tied to specific technology allows for the migration of backbone technology.
- Commercial backbone networks are implemented/maintained by network experts.

As a result, the present study begins with the assumption that network services will be transparent to the FAA end user and are provided by commercial backbone networks implemented and maintained by commercial service providers. This approach is consistent with network service offering trends as well as with FAA telecommunication contract trends (i.e. FAA Telecommunications Infrastructure^{50,51}).

Information on commercial backbone networks was solicited from several large network service providers and documented in Section 3. Each of these service providers had fairly extensive networks providing nationwide services. A figure depicting geographic network extent as well as access node locations has been provided in Section 3.1.2.1. The figure conveys the following three key characteristics of the architecture and performance of present dedicated commercial network backbones:

- High speed, high bandwidth fiber connections providing Frame Relay and ATM network services.

- Redundant paths between backbone nodes.
- Concentration of access locations around major metropolitan areas.

The first two characteristics are indicative of the ability of commercial dedicated backbone networks to satisfy the communications bandwidth and performance requirements⁵² (reliability, availability, latency) of FAA applications. A summary of the performance data obtained from commercial network service providers is provided in Table 3.1-3.

The third characteristic of present commercial network backbone networks relates to the location of network access locations also referred to as points-of-presence (POPs). Although the backbones are fairly extensive, the POPs are highly concentrated around major metropolitan areas and are more dense on the east and west coasts of the U.S. and less dense in the central region of the country. The present geographic distribution of backbone network access locations is quite different from the geographic distribution of FAA facilities, which are densely distributed in metropolitan areas, but are also uniformly distributed throughout the country. This disparity between backbone network POP locations and FAA facility distribution is the driving force behind the network access analysis. Section 4.5 is dedicated to this topic.

4.2.2 Trends

Current trends in commercial and business network services are playing a large role in influencing the trends in network backbone architecture. In general, network services can be characterized as moving towards⁵³:

- Convergence of data, voice, and video networks.
- Introduction of New Services.
- Service Bundling.

These trends in network services are driving the movement from separate voice and data network architectures to a combined backbone where data, voice and video services share a single expanded network. This convergence of services and expansion of networks is being fueled by changes in the telecommunications regulatory environment as well as the increase of data traffic. Evidence of the present and continued expansion of backbone networks can be found in the actions of large network service provider companies. For example, AT&T has noted that its focus in 2000 is scaling up for more customers and services through continued infrastructure development and leasing of unbundled network elements.⁵⁴

4.2.3 Defining Backbone Network Scenarios for Study

Section 3.1 indicates that present dedicated backbone networks extend nation-wide and have access points concentrated near major metropolitan areas. Although the exact extent of network backbones at the time of FAA implementation of a networked architecture is uncertain, growth over existing backbones is

certain. Since the potential for the growth in backbone networks and associated increase in number of POPs is large, a reasonable conclusion is that at some time in the future, all connections to a commercial backbone network will be local.

Considering present backbone architectures, network access from FAA sites to network POPs may require connections over a varying geographic distances. Technologies available and in development to accommodate these “last miles” to the FAA sites do not necessarily carry the same bandwidth and performance guarantees as the redundant, fiber backbone networks. Engineering backbone network access, therefore, was a significant activity of this study. Although details regarding access are reserved for Section 4.5, it is not hard to imagine that the availability and performance of technologies to address the “last mile” can be dependent on whether the “last mile” is truly a mile or if it is more on the order of a few hundred miles, depending on the location of the nearest network access location.

In order provide a realistic backbone network scenario for use in this study and to account for the potential substantial growth in network extent (and POPs), two backbone scenarios have been developed for this study including:

- **Low Density POP Backbone:** User current commercial backbone POP locations.
- **High Density POP Backbone:** Upper bound scenario to account for large growth potential using current Internet Service Provider (ISP) POP locations.

A description of these study scenarios is provided in the following subsections.

4.2.3.1 Low Density POP Backbone

The low density POP study scenario is a backbone network with access locations based on the current nation-wide commercial backbones deployed by major wide area network service providers. Input on current network deployment and access locations was solicited from the following service providers: AT&T, Intermedia, Qwest, MCI, and Sprint. Based on the data provided primarily by Qwest and AT&T, a combined set of POPs was developed for the Michigan and Ohio region under study (see Section 4.3.1 for selection of region under study). The combined set of POPs comprises the Low Density POP study scenario backbone access locations. These POPs are listed in Table 4.2-1.

Table 4.2-1: POPs for Low Density Backbone

<u>Michigan POPs</u>	<u>Ohio POPs</u>
Battle Creek	Akron
Birmingham	Cincinnati
Detroit	Cleveland
Plymouth	Columbus
	Toledo

4.2.3.2 High Density POP Backbone

In order to represent telecommunication network build-out trends, a second backbone study scenario was developed. This scenario represents the upper bound on network build-out. Initially, the approach to developing the upper-bound was to model the commercial backbone network and access locations on the current extent and access locations for the Internet. Upon investigation of Internet POPs for the region under study, local Internet connections (i.e. connections within the same area code and exchange) were identified for all but two FAA sites. Based on this input and the trend data, it was determined that the high density POP scenario should be a backbone network for which access from all FAA locations is via a local connection. With this case, the high-density POPs locations are the cities and towns in or near which FAA facilities are located. The high density POP locations for this study are listed in Table 4.2-2.

Table 4.2-2: POPs for High-Density Scenario

<u>Michigan POPs</u>	<u>Ohio POPs</u>	<u>Other</u>
Ypsilanti, So. Lyon, Algonac, Canton, Pontiac, Davisburg, Port Huron, Mt. Clemens, Mount Pleasant, Freeland, Litchfield, Lansing, Jackson, Romulus, Flint, Croswell, Detroit, Manchester, Carlton, Bad Axe, Ann Arbor, Alma, Ottawa Lake, Adrian	Mt. Vernon, Bluffton, Wakeman, Clyde, Luckey, Smithville, Cleveland, Elyria, Findlay, Galion, Medina, Columbia Stn., Mansfield, Marion, North Olmstead, Pemberville, Sandusky, Millbury, Swanton, Bowling Green, Oberlin	Windsor (Ontario)

4.3 ZOB FACILITIES SELECTED FOR ANALYSIS

4.3.1 Selection Process

In order to define and optimize a modern network design specific to the FAA, a subset of facilities large enough to comprise a representative set, but small enough for practical analysis was identified. The subset was selected from the ZOB ARTCC for several reasons:

- ZOB includes a large number of FAA facilities representative of a large set of different types of FAA facilities and services.
- ZOB was the subject of several previous architecture studies, and facility and requirement data from the previous studies can be directly applied.

The subset of ZOB facilities selected for analysis is shown in Figure 4.3-1.

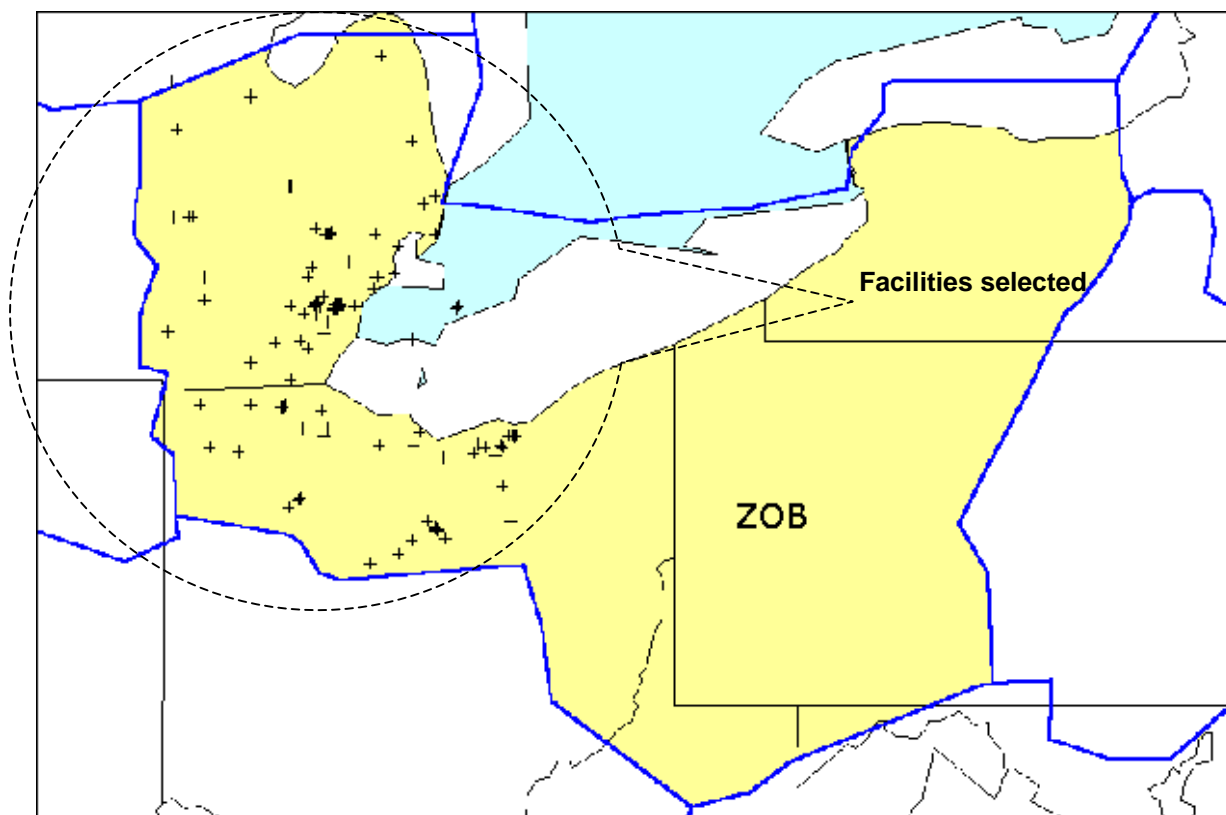


Figure 4.3-1: Subset of ZOB Facilities Selected for Analysis⁵⁵

These facilities represent a number of different FAA locations throughout Michigan and Ohio. The facilities each require some means of communication. For some, the communication requirement is simply between facilities at the same location while for others, communications between distant FAA locations are required.

4.3.2 FAA Programs Represented by the Selected Facilities

The selected facilities represent most major FAA communications utilities and programs that support air traffic control. For instance, the surveillance programs that are represented include Digitized Radar Data (RDAT), Terminal Radar Service (TRAD), and Remote Tower Alphanumeric Display (RTAD). Since FAA communication plans and budgets are presently developed relative to individual FAA programs, a table that correlates FAA programs to FAA facilities has been included in this report.

Table 4.3-1 shows the set of FAA programs that are represented by the selected facilities.

Table 4.3-1: FAA Programs Represented by Selected Facilities

Program Type	Program	Description
Automation	FSSA	Flight Service Station Automated Service
	RTAD	Remote Tower Alphanumeric Display
	RTRD	Remote Tower Radar Display
Communications (En Route and Terminal)	ATIS	Automatic Terminal Information Service
	CFCS	Central Flow Control Service
	ECOM	En Route Communications
	EFAS	En Route Flight Advisory Service
	FCOM	FSS Radio Voice Communications
	FDAT	Flight Data Service
	LABS	Leased A & B Service
	PBRF	Pilot Briefing
	SVFA	Interphone Service F (A)
	SVFB	Interphone Service F (B)
	SVFC	Interphone Service F (C)
	TCOM	Terminal Communications
FAA Communication Utilities	DMN	Data Multiplexing Network
	HCAP	High Capacity Carriers
	LINCS	Leased Interfacility NAS Communications System
	NAMS	NADIN Message Processing Service NADIN MSN
	NDNB	National Airspace Data Interchange Network NADIN PSN
	RCL	Radio Communications Link
	SAT	Satellite
Military Communication Utilities	ADIN	AUTODIN Service
	AVON	AUTOVON Service
Administrative Communications	ADDA	Administrative Data
	ADTN	Agency Data Telecommunications Network 2000
	ADVO	Administrative Voice
Other Communications	AFTN	Aeronautical Fixed Telecommunications Network
	NRCS	National Radio Communications System/Recovery Communications
	SVFD	Interphone Service F (D)
Mission Support	MNTC	Remote Maintenance Monitoring System (RMMS)
	TRNG	Training
Navigation and Landing	DIRF	Direction Finding
	ENAV	En Route Navigational Aids
	TNAV	Terminal Navigational Aids
	VNAV	Visual Navigational Aids
Surveillance	RDAT	En Route Radar Digitized Data
	RTAD	Remote Tower Alphanumeric Display Data
	TRAD	Terminal Radar Service
Weather	AWOS	Automated Weather Observing System
	ASOS	Automatic Surface Observing System
	METI	Meteorological Information
	NXRD	Next Generation Weather Radar
	RWDS	Remote Radar Weather Display Service
	TDWR	Terminal Doppler Weather Radar
Note: Some programs that utilize DMN services for transport may also be included, but are characterized under the DMN program.		

A supplement to FAA Order 1836A, Telecommunications Asset Management numbered 1830.6A and dated October 3, 1996, outlines an FAA classification of communications based on three levels of criticality. The same classification is also defined in NAS-SR-1000, Section 3.8.1.B. The classification levels are critical, essential, or routine/administrative. Availability and restoral time requirements are assigned for each of these criticality classifications. These requirements are addressed in Section 4.4.3. In addition to these categories, there have been some proposals to decompose the classification of services into a larger number of categories with more specific performance requirements.

The FAA Future Telecommunication Infrastructure (FTI) has published a set of six Reliability, Maintainability, and Availability (RMA) categories.⁵⁶ Each category has associated performance parameters including availability, restoral time, maximum outages in specified time period and maintenance service period. The FTI RMA categories and associated performance parameters are provided in Table 4.3-2.

Table 4.3-2: RMA Categories in the FAA Telecommunication Infrastructure (FTI)

RMA Parameters	RMA Category					
	RMA 1	RMA 2	RMA 3	RMA 4	RMA 5	Business Day
Maximum Number of Outages per Moving 4-month period	6	6	4	3	3	3
Maximum Number of Outages per Moving 12-month period	15	15	10	6	6	6
Maximum Restoration Time (minutes)	0.10	0.98	8.0	180	240	300
Restoral Method	Auto	Auto	Auto	Manual	Manual	Manual
Minimum Availability	0.9999971	0.9999719	0.9998478	0.9979452	0.9972603	NR
Maintenance Service Period	7x24	7x24	7x24	7x24	7x24	5x12

Although the six RMA categories above are being proposed, at the time of this study, the FAA classification of services into three criticality groups (critical, essential, and routine/administrative) is an accepted service classification. Therefore, these categories have been used to classify services carried on communications circuits within and between FAA nodes. Impact of a new service classification on communication customer premise equipment and communication links is likely to be minimal and could be addressed in the future. A list of the FAA services included in the represented architecture and their associated criticality categories is provided in Appendix A.

4.4 ZOB NODES DEFINITION AND COMMUNICATION REQUIREMENTS

4.4.1 Grouping ZOB Facilities into Nodes

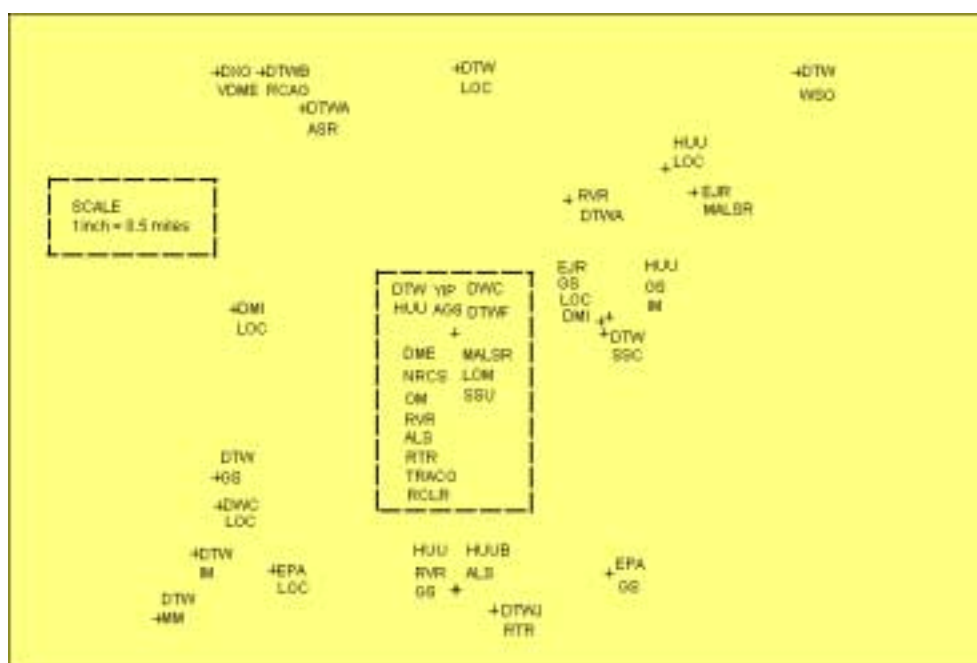
An FAA site may consist of a single or group of FAA facilities. Each facility performs a function that may require only local communication with other facilities on the premises, or may require

communication with a distant FAA facility. In this study, a **node** is defined for each FAA site that includes facilities requiring communications with distant FAA facilities (i.e. at a different FAA location). The process of defining FAA network nodes for the ZOB representative architecture consisted the following several steps:

1. Identify FAA facility Location Identifiers (LIDs) and corresponding FAA facilities.
2. Identify geographic location of each LID/facility pair (address, latitude, longitude).
3. Create a map to provide a graphical description of each LID/facility pair.
4. Utilizing address, latitude, and longitude information in addition to FAA facility maps and other data, group LID/facility pairs into potential FAA node sites (facilities had to be within three to five nautical miles to be considered as a single node).
5. For each potential node site, determine if the facilities at the location require communications with a facility at a different FAA location; if so, the site is defined as a FAA node.

Information from the FAA Telecommunications Information Management System (TIMS) database and the National Flight Data Center was utilized to perform these steps. The TIMS database describes all FAA leased circuits, including terminating facility information, derived from Defense Information Technology Contracting Organization (DITCO) billing tables. Queries against the TIMS database provided address, latitude and longitude information for each facility. This geographic information, along with information from the National Flight Data Center, was used as input to mapping software to create FAA facility maps. A sample map for the region around the Detroit Metropolitan Airport is provided in Figure 4.4-1. This figure shows FAA facilities collocated on a single property (e.g. airport) as well as remote, standalone facilities. Facilities are shown with corresponding LID designation.

Using the methodology described above, the several hundred FAA facilities selected for inclusion in the representative architecture were reviewed and grouped into FAA network nodes. The resulting set of nodes for the representative architecture is identified in Table 4.4-1.



4.4.2 Local Node Communications

Many of the nodes and associated communication lines identified in the study accommodate legacy FAA systems not equipped to directly connect to a networked communication system. In order to migrate existing communication circuits to a modern network architecture, several changes need to be implemented at the FAA nodes. These changes included:

- Addition of gateways to provide a mapping of legacy FAA equipment protocols to networked protocols.
- Replacement and/or re-allocation of existing modems, Data Service Unit (DSU)/Channel Service Unit (CSU), switches and other communication equipment with network switching and network routing edge devices to route communications within a node and provide the connection to the backbone network.
- Replacement of existing multiple point-to-point leased lines and FAA-owned cables with new communication lines or cables, which interconnect network devices.
- Addition of enterprise management software and security functions.

In the advent of new telecommunication service contracts for the FAA, these changes, which would include the implementation of new equipment, network management, and security, would be wrapped into the contracted services. For example, if IP services were negotiated, the Service Provider would be responsible for selection, implementation, operation, and maintenance of customer premise network equipment (including switching and routing devices).

Table 4.4-1: FAA Network Nodes for the Representative Architecture

Node #	Node ID	FAA Location ID (LID)	FAA Facility Type (FAC)	Address
1	AA8	AA8	RCLR	Wakeman, OH
2	AB8	AB8	RCLR	Clyde, OH
3	AC8	AC8	RCLR	Luckey, OH
4	ADG	ADG	ASOS	Adrian, MI
5	AE8	AE8	RCLR	Ottawa Lake, MI
6	AMN	AMN	RTR	Alma, MI
7	ARB	ARB, ARBZ	ATCT, RTR	Ann Arbor, MI
		AH8	RCLR	Ann Arbor, MI
8	BAX	BAX	RCO	Bad Axe, MI
9	BJJ	BJJ	ASOS, RCO	Smithville, OH
10	CLE	CLE	TDWR, AFSS, WSFO, TRAON, ARPT, ASOS, RTR, FSDO, MIDO, CASFU, SSU, OM, ARSR, BUEC	Cleveland, OH
11	CRL	CRL	VTAC, RCO, RCAG, BUEC	Carlton, MI
12	DET-1	DET	IBP	Manchester, MI
13	DET-2	DET, DETA, DETB, DETC	RCO, SSU, ATCT, RTR, LOC, VOT, ASOS	Detroit, MI
14	DFI	DFI	ASOS	Defiance, OH
15	DJB	DJB	RTR, RCO, VTAC	Elvria, OH
		CLE	VOT	Elvria, OH
		22G	ARPT, ASOS	Elvria, OH
16	ECK	ECK	RCO, VTAC	Crosswell, MI
17	FDY	FDY, FDYA	RCO, RCAG, BUEC, VTAC, RTR, DF, ASOS, AWOS	Findlay, OH
18	FNT	FNT, FNTA, FNTB	TRACON, SSC, WSO, RCO, GS, RCAG, VTAC, RTR, LOM	Flint, MI
19	GQQ	GQQ	RTR	Gedion, OH
20	HE8	HE8	RCLR	Medina, OH
21	ID8	ID8	RCLR	Columbia Stn, OH
22	DTW/HUU	AG8	RCLR	Romulus, MI
		DMI	GS, MALSR, LOC, OM, LOM	Romulus/SouthGate, MI
		DTW	ASR, OM, NRCS, RTR, GS, SSC, TRACON, RCAG, DME, LOC, IM, CASFU, ALS, RVR, MM, RVR	Romulus, MI
		DXO	VDME	Romulus, MI
		DWC	LOC	Detroit, MI
		EJR	GS, LOC	Romulus, MI
		EPA	LOC, GS	Romulus, MI
		HUU	OM, LOC, IM, MM, GS, ALS	Romulus, MI
23	JXN	JXN, JXNA, JXNB	RCO, ATCT, NRCS, RTR, VDME	Jackson, MI
24	LAN	LAN	VTAC, SSU, AFSS, TRACON	Lansing, MI
		CPQ	LOC	Lansing, MI
25	LFD	LFD	BUEC, RCAG, RCO	Litchfield, MI
26	MBS	MBS, MBSA	RCAG, RTR, TRACON, BUEC, VDME	Freeland, MI
27	MFD	MFD, MFDA, MFDB	LOC, GS, RCO, VTAC, RTR, BASOP, TRACON, WSO, RCAG	Mansfield, OH
28	MNN	MNN	ASOS, RTR	Marion, OH
29	MOP	MOP	VDME	Mt. Pleasant, OH

Table 4.4-1: FAA Network Nodes for the Representative Architecture (Cont'd)

Node #	Node ID	FAA Location ID (LID)	FAA Facility Type (FAC)	Address
30	MTC	MTC	ATCT, BASOP	Mt. Clemens, MI
31	OHI	OHI	SMO	N. Olmstead, OH
32	PHN	PHN	LOC, ARPT	Port Huron, MI
33	PSI	PSI	BUEC, VTAC, RCO	Davisburg, MI
34	PTK	PTK, PTKA	ATCT, GS, RTR, LOC	Pontiac, MI
35	QD4	QD4	RTR	Pemberville, OH
36	QDT	QDT	SSU, ARSR	Canton, MI
37	QTA	QTA	RCAG	Algonac, MI
38	SKY-1	SKY	RCAG	Sandusky, OH
39	SKY-2	SKY, SKYA	RCO, VTAC	Sandusky, OH
40	SVM	SVM	RCO, VTAC	So. Lyon, MI
41	TDZ	TDZ	ASOS	Millburg, OH
42	TOL	TOL	BASOP, ANGB, ASR, TRACON, RTR	Swanton, OH
43	VWV	VWV	RCAG, RCO, VDME	Bowling Green, OH
44	YIP	YIP	ATCT, SSU, FSDO, SMO, TDWR, WSO	Ypsilanti, MI
		DTW	FSDO, WSO, TDWR	Belleville, MI
45	YQG	YQG	ATCT	Windsor, Ontario
46	ZOB	ZOB	ARTCC	Oberlin, OH
47	5G7	5G7	ATOVN	Bluffton, OH
48	4I3	4I3	RTR	Mt. Vernon, OH

To effectively use the services provided in new telecommunication service contracts, the systems and equipment at FAA nodes must be considered together as a single entity or network, with specific sub-networks that have specific communication performance requirements. This approach requires a coordinated approach of determining overall telecommunication needs to avoid continued use of a telecommunication service contract to support point-to-point connections and to allow for purchase of bulk bandwidth, increased utilization of communication links, and cost savings benefits.

4.4.2.1 Campus Network Development Methodology

As outlined in the general approach described above, each FAA node was defined as a “campus” comprising one or more FAA sites. A procedure for identifying key campus network elements was developed, using a methodology recommended for the design of a modern IP network.⁵⁷ This methodology is a top-down approach with the network design following the typical protocol stack. First, different applications and systems with communication requirements were identified for different types of FAA facilities. Applications were allocated to functional groups that would share common communication resources within a node, depending on the application type and their associated performance requirements, including availability, diversity, network response time, end-to-end delay and delay jitter. These common communication resources would then all interface to a campus router, which provides the external interface for the node.

Three broad categories of FAA nodes were considered for application of the campus network development approach. These included:

- Nodes with TRACONs or Towers.

- ARTCCs.
- Nodes comprising remote FAA equipment and facilities.

Specific campus area network development approaches for each category of node are described in Section 4.4.2.2. These concepts were applied to the FAA nodes under analysis. Where applicable, current FAA local area network projects and plans were considered for the nodes during the development of the campus networks.

4.4.2.2 Campus Area Network Concepts

The following subsections describe the campus network architecture concepts developed and applied to the ZOB nodes included in the study.

4.4.2.2.1 Campus Networks for TRACONs/Towers

FAA TRACONs and Towers considered in the study utilize a variety of systems to support operational and administrative functions. These systems were grouped into broad groups generally following the organization NAS telecommunication services in the Aviation System Capital Investment Plan (CIP), 2000 Future Telecommunications Plan (Fuchsia Book), and 1999 Currant FAA Telecommunication Systems and Facility Description Manual (Currant Book). A summary of the communication groups and associated FAA services, facilities and end-systems is provided in Table 4.4-2.

Table 4.4-2: TRACON/Tower Communication Groups

Communication Group	Services	Associated FAA Facilities/End Systems
Automation and Operational Data Communications	FSSA, RTAD/RTRD, CFCS, FDAT, IDAT	Flight Service Data Processing System, Flight Service Automation System, DBRITE, Traffic Management Unit, Flight Data Input/Output Remote, ARTS
Critical Operational Voice Communications	ECOM, TCOM, NRCS	RCAG, BUEC, VSCS, Air Traffic Control Position (ATCP), RTR
Non-critical Operational Voice and Data Communications	ATIS, CFCS, EFAS, FCOM, PBRF, AFTN	ATIS Recorder, RTR, VOR/DME, VOR, VORTAC, Operational Voice Switch for Traffic Management, Traffic Management Unit, Flight Service Specialist Position (FSSP), RCO, Pilot's Automatic Telephone Weather Answering System, Maintenance Data Terminal, Maintenance Processing System, Dynamic Simulator, Electronic Target Generator
Administrative Voice and Data Communications	ADTN, ADDA, TRNG, ADVO	PBX, Computer Terminal, Telephone, PBX, Fax, Computer Based Instruction unit,
Navigation and Landing Systems	DIRF, ENAV, TNAV, VNAV	VOR, DME, TACAN, LOM, GS, IM, MM, OM, Direction Finder Indicator, Direction Finder, Navigation Monitor and Control, Remote Maintenance Concentrator, RVR, RVR Data Processing Unit
Surveillance Data	RDAT, TRAD	ARSR, ATCBI, ASR, ATCBR, ARTS,
Weather	ASOS, AWOS, ATIS, METI, NXRD, RWDS, TDWR	ASOS, AWOS, PSTN, ATIS Recorder, VOR/RTR, AWOS Data Acquisition System, GOES terminal, Airport Weather Information System (AWIS)

The general approach for campus network architecture for TRACONs and tower nodes was to create a dedicated LAN for each communication group as defined above. For cases where a stand-alone LAN for a particular group was not warranted due to the small number of end-systems in a particular group, groups with similar performance requirements could share LAN equipment, or the campus router could be used to satisfy local network requirements. High-level block diagrams of the LAN architectures for the various communication groups are provided in Figure 4.4-2.

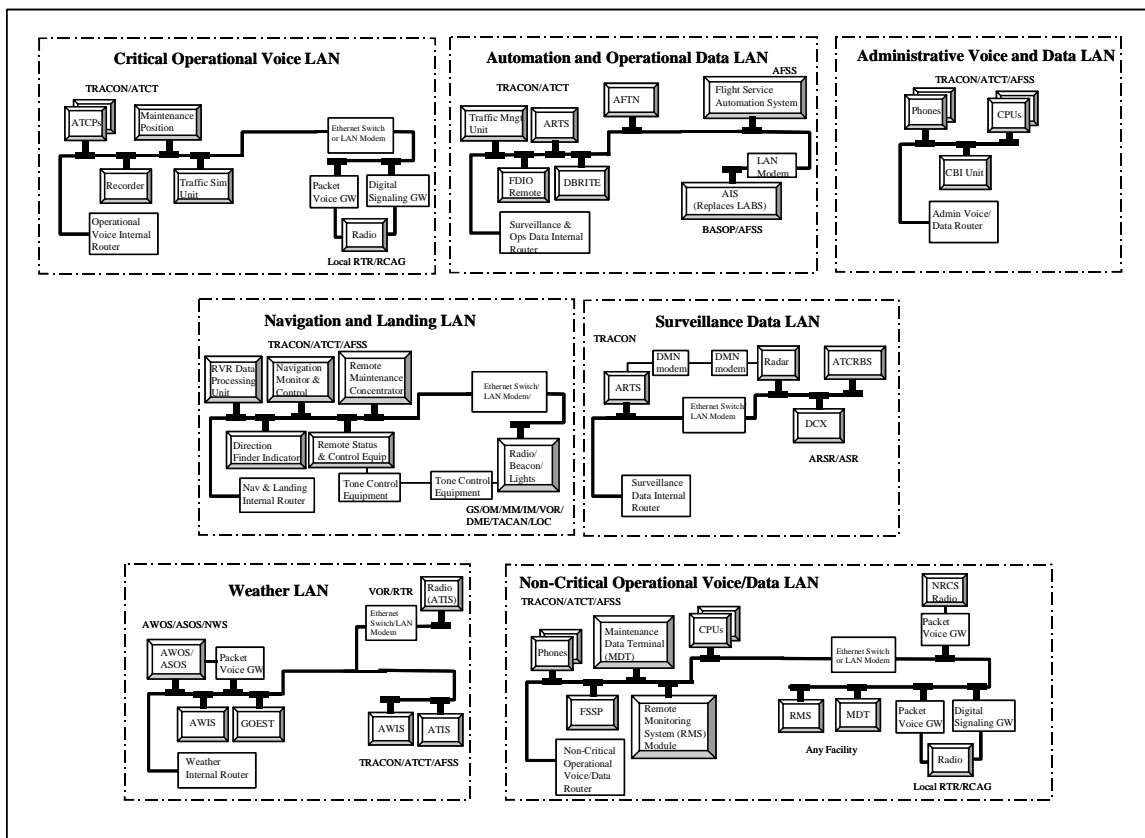


Figure 4.4-2: TRACON/ATCT Campus Area Network Components

Individual component LANs were then connected to a single campus router or series of campus routers that provide the external interface for the FAA nodes.

Nodes with external connections carrying critical FAA services included a screened-subnet firewall implementing VPN Functionality. It included a campus (internal) router; a bastion-host server and firewall providing a DMZ; and a dedicated external connection router. These security configurations have been discussed in Sections 2.2 and 3.3.

4.4.2.2.2 Campus Networks for ARTCCs

The ARTCC facility included in the study was ZOB (Cleveland). This facility has several existing LANs to service different FAA end-systems. These LANs include:

- URET/EDI LAN
- DSR LAN
- NAS LAN
- AIS LAN
- CTAS LAN
- ATM/TFM LAN

The approach for the intra-facility communications architecture for ZOB was 1) to maintain the existing LAN structure, with LANs interfacing with a campus (edge) router, and 2) create new LANs for systems that do not currently provide a routable interface to external communication. New LANs within an ARTCC included:

- Weather Processing
- Surveillance Processing
- Critical Operational Voice Communications
- Maintenance Processing
- Operational Voice Communications
- Administrative Voice and Data Communications

As a result of the new architecture, existing and proposed LANs would interface to one or more common campus routers that would provide the interface to external communications. Interfaces to the Administrative Data Transmission Network (ADTN) were maintained, while interfaces to the National Airspace Data Interchange Network (NADIN), Packet Switched Network (PSN), and Bandwidth Manager (BWM) networks would be migrated to the new IP service network. A large number of communications with an ARTCC include critical traffic, therefore a DMZ was established at the external communication interface. A high-level block diagram of the resulting ARTCC campus network is provided in Figure 4.4-3.

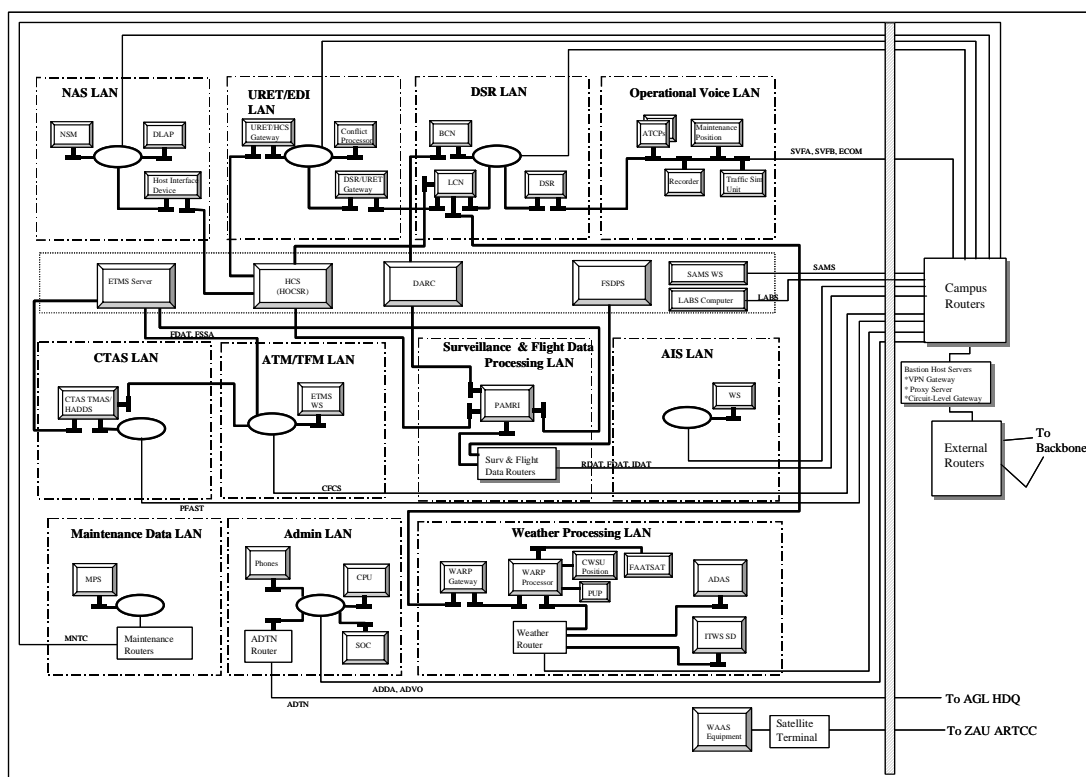


Figure 4.4-3: ARTCC Campus Network

4.4.2.2.3 Campus Networks for Remote FAA Nodes

FAA nodes classified as remote are primarily un-manned locations that support equipment such as radars, A/G radios, weather measurement equipment, and navigation equipment. A small manned facility with a small number of communication end-systems was also classified as remote. Due to the limited number of FAA systems at remote sites, implementation of separate physical LANs for each different functional category of FAA service would not be cost effective.

Because of the high priority and criticality of operational voice services and radar services located at remote sites, dedicated network resources were maintained for those services. For all other equipment, a single dedicated network was implemented with software (e.g. Virtual LAN (VLAN)) addressing separate service local communication requirements. A single exception to this approach was to include local administrative/routine voice circuits located at a remote air/ground radio (RCAG/BUEC/RTR) site on the same physical local area network as the A/G voice traffic, but with lower network priority.

4.4.3 Bandwidth and QoS Constraints by Node

With the implementation of a campus area network for each node, connections to the backbone network would consist of a single primary connection and, where required to meet performance requirements, redundant connections to the backbone network. To define the size and type of connection to the backbone network, the bandwidth and QoS constraint of each node is required. These parameters influence the technology of the backbone access connection as well as the number of connections, both of

which are cost driving parameters. In the advent of new FAA telecommunication service contracts, these parameters would be important components of a SLA (See Sections 2.1 and 3.1.2.1). In this study, these parameters were also used to identify backbone access technologies and quantities of connections to the backbone network as part of the cost analysis (See Section 5.4).

To derive bandwidth and QoS constraints for each node, the characteristics of the individual FAA facilities located within a node were identified. For many of the FAA facilities, communication requirements were derived in previous architecture studies⁵⁸. For other facilities not addressed in previous studies, communication requirements were derived using several references, including:

- *Current FAA Telecommunications System and Facility Description Manual, Currant Book*, Fiscal Year 1999 Edition, NAS Operations (AOP) Telecommunications Support and International Communications Division
- *Future FAA Telecommunications Plan, Fuschia Book*, NAS Operations (AOP) Telecommunications Network Planning and Engineering Division, April 2000.
- NAS-SS-1000
- NAS-SR-1000
- *FAA NAS System Requirements Document FAA Order 6000.36*, Communication Diversity for NAS Services
- *FAA Telecommunication Infrastructure Investment Analysis Report*, July 13, 1999
- *FAA TIMS Database*, April 2000 download
- *NAS Communications Architecture – Design Alternatives*, Stanford Telecom, TR98083, November 1, 1998.
- *En Route Surveillance Architecture and Tracking Study*, Stanford Telecom, TR99009, May 1999.
- *Automation System Communication Requirements*, Stanford Telecom, TR99004, May 1999.

4.4.3.1 Bandwidth Determination by Node

Using these resources, bandwidth requirements for each specific FAA services and facilities were identified. Based upon the nature of the service, number and type of communication lines, service descriptions provided in the Currant Book and Fuchsia Book, previous communication architecture studies, and packet-voice analysis as described in Section 2.2 and Section 3.2, specific bandwidth requirements for all facilities that comprise a node were calculated.

Calculations were made under worst-case, maximum data rate conditions for each node connecting to the backbone network. These conditions assumed instantaneous maximum utilization of all services within a node. The resulting peak instantaneous bandwidth into a node and peak instantaneous bandwidth out of a node are provided in Table 4.4-3. Nodes not included in the table *do not connect to the backbone network* (Reference Section 4.5.1)⁵⁹. Since an overwhelming majority of end-systems interfacing with the proposed network equipment are legacy systems, margin was added to the bandwidth calculations to

account for encapsulation of data into network IP packets. The 20% margin also accounted for the flow of management, security, and digital signaling data in the network.

Table 4.4-3: Peak Instantaneous Node Bandwidth Requirements

Node #	Node	Location	Node NXX/NPX	Peak Instantaneous BW In (20% margin) (kbps)	Peak Instantaneous BW Out (20% margin) (kbps)
4	ADG	Adrian MI	517/265	13.44	16.32
6	AMN	Alma MI	517/463	13.44	13.44
7	ARB	Ann Arbor MI	734/973	204.48	209.52
8	BAX	Bad Axe MI	517/269	13.44	13.44
9	BJJ	Smithville OH	330/669	26.88	29.76
10	CLE	Cleveland OH	216/265	1777.92	1792.32
11	CRL	Carlton MI	313/584	94.08	94.08
12	DET-1	Manchester MI	734/428	46.08	46.08
13	DET-2	Detroit MI	313/521	2124.48	26.52
14	DFI	Defiance OH	419/658	13.44	16.32
15	DJB	Elyria OH	440/322	53.76	56.64
16	ECK	Croswell MI	810/679	26.88	26.88
17	FDY	Findlay OH	419/422	161.28	164.16
18	FNT	Flint MI	810/238	426.24	426.24
19	GQQ	Galion OH	419/684	13.44	13.44
22	DTW/HUU	Romulus MI	734/941	6104.64	6078.72
23	JXN	Jackson MI	517/782	108.48	111.36
24	LAN	Lansing MI	517/321	1474.56	1463.04
25	LFD	Litchfield MI	517/542	107.52	107.52
26	MBS	Freeland MI	517/695	404.16	407.04
27	MFD	Mansfield OH	419/522	428.16	431.04
28	MNN	Marion OH	740/382	26.88	29.76
29	MOP	Mount Pleasant MI	517/772	29.76	29.76
30	MTC	Mt. Clemens MI	810/465	67.2	67.2
32	PHN	Port Huron MI	810/364	2.88	2.88
33	PSI	Davisburg MI	248/625	53.76	53.76
34	PTK	Pontiac MI	248/666	2308.8	450.24
35	QD4	Pemberville OH	419/865	13.44	13.44
36	QDT	Canton MI	734/942	84.48	84.48
37	QTA	Algonac MI	810/765	94.08	94.08
38	SKY-1	Sandusky OH	419/359	67.2	67.2
39	SKY-2	Sandusky OH	419/626	26.88	26.88
40	SVM	So Lyon MI	810/437	29.76	29.76
41	TDZ	Millbury OH	419/838	13.44	16.32
42	TOL	Swanton OH	419/865	334.08	336.96
43	VWV	Bowling Green OH	419/352	40.32	40.32
44	YIP	Ypsilanti MI	347/482	560.64	534.72
45	YQG	Windsor Ontario	516/?	13.44	13.44
46	ZOB	Oberlin OH	216/774	8205.6	8205.6
48	4I3	Mt. Vernon OH	740/397	13.44	13.44

4.4.3.2 Latency Determination by Node

Latency requirements did not apply to the FAA node as a whole, but rather to the individual facilities and services within a node. As described in the *NAS Architecture Vision for the Communications Area*,⁶⁰ latency goals and requirements are difficult to identify. This is due to the varying means in which latency is addressed in FAA performance requirements documents, and at times, the lack of guidance in these documents. The *NAS Architecture Vision for the Communication Area* report outlines methodologies for identifying latency goals for both voice and data systems and specific latency values. The latency values derived in that report are also used in this study and are summarized in Table 4.4-4.

Table 4.4-4: Latency Constraints Based on Service

Service	Latency Allocation (ms)	
Data	<u>Critical</u> ¹ 300	<u>Essential Routine</u> ² 600
Operational Voice	Initiation of <u>one-way tx</u> ³ 250	End-to-End <u>Calculated</u> ⁴ 150
Administrative Voice	300 ms ⁵	
<div>1. Based on the communication latency for radar data in NAS-SS-1000 Volume I, pg. 58 and NAS-SR-1000 Section 3.2.1.2.7.1.1, Table 3.2.1.2.7.1.1-1 (Radar Data Response Specification).</div> <div>2. NAS-SR-1000 Volume IV, pg. 3-152 provides range of latency from 600 ms to 10 s, depending on the service. The most conservative value is used.</div> <div>3. NAS-SR-1000 Section 3.6.1.A.5.a (Voice Response Specification).</div> <div>4. Calculation including voice switching equipment specification (VSCS specification) and transmission equipment specification (NAS-SS-1000 Volume IV, p. 93, Section 3.2.1.4.1.2.2).</div> <div>5. Derived based on International Telecommunication Union (ITU) recommendation on Telephone Transmission Quality.</div>		

4.4.3.3 Availability Determination by Node

Similar to latency requirements, availability requirements are associated with specific FAA facilities and services compared to general node requirements. As discussed earlier in Section 3.1.1.2, specific availability requirement values are clearly specified in FAA requirement documents based on the FAA service criticality classification. End-to-end availability and associated restoral times are provided in NAS-SR-1000, Section 3.8.1B, and in Table 4.4-5 below.

Table 4.4-5: Availability and Restoral Time Requirements for NAS Services

Service	Availability	Restoral Time
Critical	0.99999	6 seconds
Essential	0.999	10 minutes
Routine	0.99	1.68 hours

4.4.3.4 Diversity Determination by Node

A final QoS parameter addressed is diversity. FAA Order 6000.36A, *Communication Diversity*, identifies FAA critical services that require communication diversity. Included in the order is an appendix outlining the various means by which diversity can be accomplished. These include redundant (diverse) communication paths to a single facility as well as the use of two diverse facilities for common transmission capability. To maintain a consistent level of comparison among proposed architectures developed in this study and the baseline architecture, the following assumption was made: if redundant connections/equipment are, or could be, used at a particular FAA facility for the baseline architecture, redundancy in equipment and connections was also included in the proposed architectures.

4.5 CONNECTING NODES TO BACKBONE NETWORKS

4.5.1 General Architecture Concepts

The general vision for the architecture concepts developed in this study is provided in Section 4.1. This vision includes the use of leased WAN services as the backbone of the architecture, and interfacing of both legacy (networked and non-networked) and new standard users to the backbone. Three specific architecture scenarios have been developed to address both the general architecture vision, and the specific requirements of existing FAA facilities and systems. The scenarios are related to the topology of the backbone network (as described in Section 4.2.3) and the way in which FAA nodes access the backbone. The scenarios include:

- Scenario 1A: All nodes connect directly to a low-density POP backbone
- Scenario 1B: Regional FAA hubs connect to a low-density POP backbone
- Scenario 2: All nodes connect directly to a high-density POP backbone

The first two scenarios are related in that both utilize the low-density POP backbone. The difference between the two scenarios is how the nodes access the backbone. For Scenario 2, only a single access scheme is used. Each proposed architecture is described in the following subsections.

4.5.1.1 Scenario 1A: All Nodes Connect Directly to the Low-Density POP Backbone

Scenario 1A follows the low-density POP backbone scenario, where backbone access locations in the ZOB region include four locations in Michigan and five locations in Ohio (reference Table 4.2-1). All external connections for FAA nodes are made to the closest backbone access location. For some FAA nodes, the geographic distance to the nearest POP is very small; however, for many nodes, this connection is across a large geographic distance, perhaps significantly longer than the baseline connections. A depiction of this architecture is provided in Figure 4.5-1. Note that only the backbone POPs and not the backbone itself are provided in the figure. The backbone would include redundant interconnection of these POPs and other backbone routers.

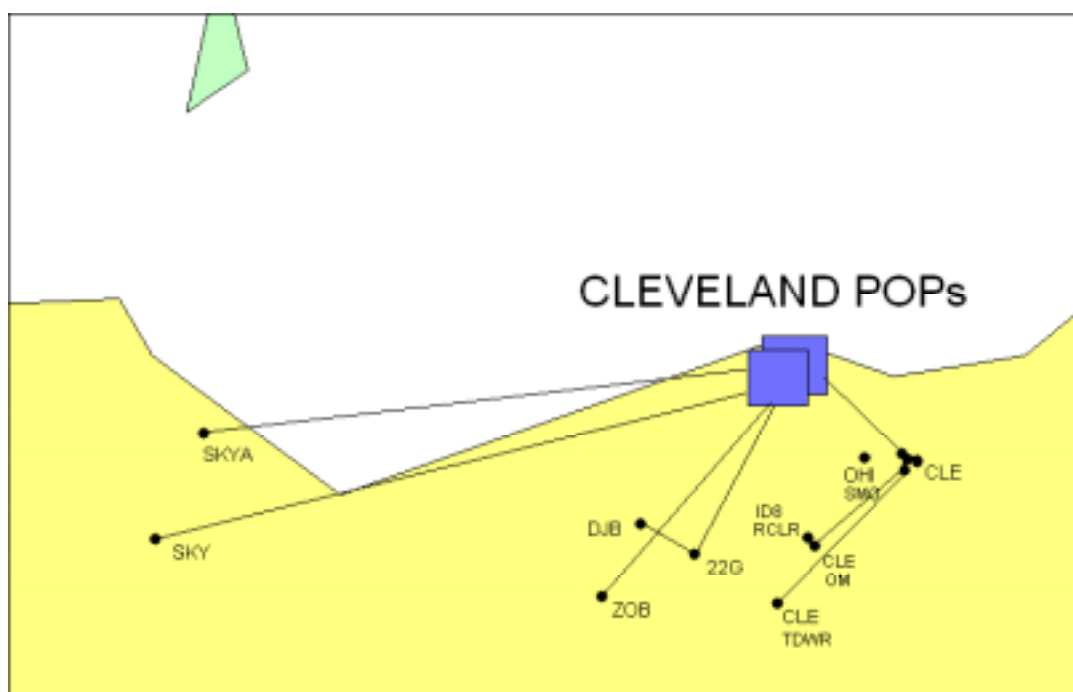


Figure 4.5-1: Architecture Scenario 1A Node Connections

This architecture represents the current state of commercial wide-area-network deployment for leased IP network services. Scenario 1A maximizes the bandwidth aggregation at large nodes by having only a single connection point for the nodes, namely the nearest POP. This aggregation, as well as the utilization of all-digital networked communications, allows for the leasing of bulk bandwidth.

Because there is a large geographic distance between many of the FAA nodes and the closest backbone POP location, some of the bandwidth aggregation cost savings may be outweighed by backbone access cost increases. Specific cost impact is investigated as part of the cost analysis of Section 5.4.

4.5.1.2 Scenario 1B: Regional FAA Hubs Connect to a Low-Density POP Backbone

Similar to Scenario 1A, the architecture for Scenario 1B used the backbone network access locations listed in Table 4.2-1 for the low-density POP backbone. Due to the large-geographic distance between many of the FAA nodes and the closest backbone POP location, an architecture which included regional area networks with a single connection path between the regional network and backbone network was developed. This concept features hub and spoke type regional networks with large TRACONs and ARTCCs at the hub locations. The hub locations have a direct aggregated bandwidth connection to the backbone network. The remote or smaller facilities have dedicated leased connections to the nearest FAA hub. In general, these connections were smaller in geographic distance than the connections to the closest POP. Figure 4.5-2 depicts this architecture scenario. As before, note that only the backbone POPs and not the backbone itself are provided in the figure. The backbone would include redundant interconnection of these POPs and other backbone routers.

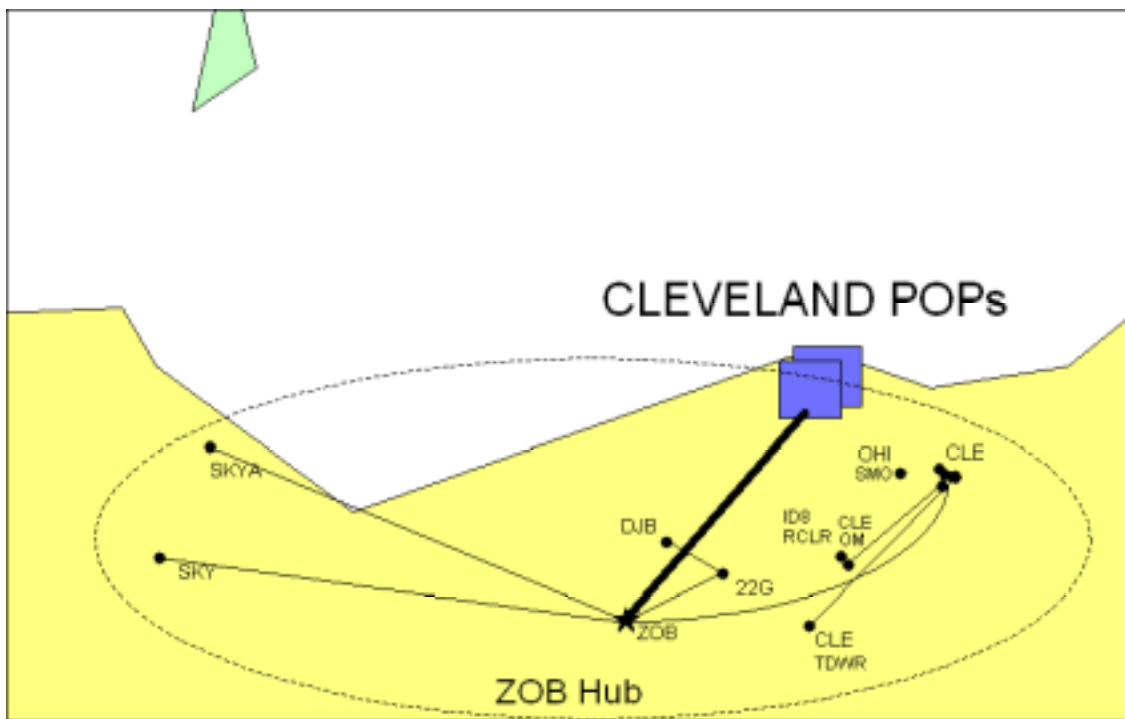


Figure 4.5-2: Architecture Scenario 1B Node Connections

Similar to Scenario 1A, the current deployment of leased WAN IP service networks is reflected in this architecture. Additionally, the architecture provides for the substantial aggregation of bandwidth at a large TRACON or ARTCC for connection to the network backbone. A recent characterization of existing FAA circuits in the ZOB region⁶¹ showed that communications among large and medium facilities account for as much as 74% of total leased communications costs. Architecture Scenario 1B therefore would likely provide significant bandwidth efficiency and potentially higher backbone access cost efficiency than Scenario 1A.

The cost impact of the loss of some bandwidth efficiency between Scenario 1A and 1B is addressed in the cost analysis of Section 5.4. Another potential impact of this architecture is the slightly more complex network management as a mix of dedicated and networked communication services are used.

4.5.1.3 Architecture Scenario 2: Connecting All Nodes Directly to the High-Density POP Backbone

The third architecture scenario is structured around the high-density POP backbone network. This network is reflective of trends in WAN deployment as well as cooperation among service providers to provide seamless WAN services. In this scenario all FAA nodes can access the backbone via a local connection. Because this scenario allows for maximum bandwidth aggregation at large FAA nodes as well as short geographic distance (lower cost) backbone access connections, there was no justification to develop any alternatives to direct backbone connection for the high density POP case.

Although this scenario maximizes cost efficiencies in terms of bandwidth and backbone access connections, there is a risk specific to this architecture scenario in regard to forecasted commercial WAN growth. Although trend reports expect substantial expansion of WANs, expansion may be focused in certain geographic regions and may take considerable time. These concepts and the WAN expansion realization risk need to be considered when comparing this architecture scenario to the other two.

4.5.2 Connection Technology

In the representative architectures developed in this study, it is envisioned that a single SLA between a service provider and the FAA would cover all aspects of IP network services. This not only would include customer premise equipment and backbone services, but also connection of the FAA node to the backbone network. Because these types of full service packages are not currently available, understanding performance and cost parameters requires investigation of what components comprise a full service package. The backbone network service component was addressed in Section 3. This section and associated subsections address connection of the FAA nodes to the backbone network. The third component of the full service package, customer premise equipment, is addressed in Section 4.6.

4.5.2.1 Existing Technology and Trends

With the development of high bandwidth applications such as video-on-demand and interactive television (TV), and the expansion of high bandwidth backbone networks has come substantial development of various technologies for accessing backbone networks. New and emerging technologies are expanding the bandwidth barriers of today's technologies and exploiting the true potential bandwidths of a variety of physical media including copper twisted-pair, coaxial cable, optical fiber, and radio frequency (RF) in space. Although the future success of these technologies will depend on availability, pricing, ease of installing, and relevant applications supported, general consensus in the business and technical communities is that a single technology will not dominate. Rather, different access technologies will dominate specific applications.

For this study, a set of technologies that are representative of current and future means of network access are considered in the context of applicability of connecting ZOB nodes to a backbone network. These technologies include both mature and fully deployed technologies as well as those technologies in the final stages of standardization, development, and deployment. A summary of these representative technologies is provided in Table 4.5-1.

Table 4.5-1: Summary of Considered Access Technologies

Network Access Technology	Speed	Physical Medium	Typical Applications
Analog Modem using POTS	Up to 56 Kbps	Twisted-pair	Home and small business access
DS0 DS1/T-1 DS1C/T-1C DS2/T-2 DS3/T-3	64 Kbps 1.544 Mbps 3.152 Mbps 6.312 Mbps 44.736 Mbps	Twisted-pair, coaxial cable, or optical fiber	Large company to ISP; ISP to Internet infrastructure; for DS3, smaller links within Internet infrastructure
ISDN	BRI: 64 -128 Kbps PRI: 23 (T-1) assignable 64-Kbps channels plus control	BRI: Twisted-pair PRI: T-1 or E1 line	BRI: Faster home and small business access PRI: Medium and large enterprise access
3G Cellular and Terrestrial Wireless including LMDS and MMDS	Up to 2 Mb/s (3G) Up to 36 Mb/s (shared for LMDS)	RF in space (wireless)	Mobile telephone for business and personal use
Satellite	400 Kbps (DirectPC) Up to 16 Mbps (Spaceway) Up to 64 Mbps (Teledesic)	RF in space (wireless)	Faster home/small enterprise access; high speed internet; multimedia
Frame relay	56 Kbps to T3	Twisted-pair or coaxial cable	Large company backbone for LANs to ISP; ISP to Internet infrastructure
Digital Subscriber Line (DSL)	512 Kbps to 8 Mbps	Twisted-pair	Home, small business, and enterprise access using existing copper lines
Cable modem	512 Kbps to 52 Mbps (shared) (see Key below)	Coaxial cable	Home, business, school access
Fiber/PON	155 Mbps (see Key below)	Optical fiber	ISP to Internet infrastructure Smaller links within Internet infrastructure
<p>Key: "T" = T-carrier system in U.S., Canada, and Japan carrier). "DS"= digital signal (that travels on the T-carrier).</p> <p>Only the most common technologies are shown. "Physical medium" is stated generally and doesn't specify the classes or numbers of pairs of twisted pair or whether optical fiber is single-mode or multimode. The effective distance of a technology is not shown. There are published standards for many of these technologies.</p> <p>Cable modem note: The upper limit of 52 Mbps on a cable is to an ISP, not currently to an individual PC. Most of today's PCs are limited by an internal design that can accommodate no more than 10 Mbps (although the PCI bus itself carries data at a faster speed). The 52 Mbps cable channel is subdivided among individual users. Obviously, the faster the channel, the fewer channels an ISP will require and the lower the cost to support an individual user.</p> <p>The Full Services Access Networks Consortium (FSCA) has developed a PON specification for supporting fiber to the home (FTTH), fiber to the building (FTTB), Fiber to the Curb (FTTC) etc. This specification includes 155 Mbps upstream and 155 Mbps downstream data rates.</p>			

The technologies listed in the table encompass the current range of technologies considered in the U.S. for both present and future network access.

Although Fiber/Passive Optical Network (PON), Cable Modem and ISDN satisfy access requirements for some or all nodes, these technologies were not included in the representative architecture. Fiber/PON has significant potential to become a universal access technology, however it is a longer-term future solution as its deployment requires substantial capital. Cable modems may provide significant bandwidth at attractive prices. However, traditional topologies do not support FAA availability requirements, and infrastructure upgrade is incremental due to cost constraints. Finally, although ISDN has good market share today, certain technology limitations as well as the potential of alternative technologies have led to the perception that ISDN will not be a significant access technology of the future.

Terrestrial wireless and broadband satellite technologies have been forecasted to see considerable growth and availability in the future. Although not considered in this study as a primary access technology, as these technologies mature, they may be very suitable candidates for diverse access as well as primary technologies in certain locations.

The remaining technologies are all widely available or show considered expansion and should meet FAA requirements at particular nodes. In an effort to select a single primary access technology to use in the representative architecture development and cost analysis, it is assumed that all primary access connections are made using standard Direct Digital Connectivity (DDC) services. Specific lines have been selected according to the bandwidth constraints for the nodes.

4.6 NETWORK EQUIPMENT AT FAA NODES AND NETWORK CIRCUITS

Network equipment at the ZOB nodes includes the customer premise equipment to provide campus area networking among node facilities and the external connection of the node to the backbone network or to other nodes. The specific requirements for network equipment at the nodes depends significantly on the campus area network developed for the node as discussed in Section 4.4.2.2. Additionally, the size and redundancy of the external node communication connections are a reflection of the bandwidth and QoS constraints for the node as addressed in Section 4.4.3. Application of the methodologies and analysis of Section 4.4.2.2 and Section 4.4.3 is addressed in the following subsections.

4.6.1 Customer Premise Equipment

The campus area network design concepts discussed in Section 4.4.2.2 were applied to each of the nodes in the representative architectures. A set of functional equipment block diagrams was created to reflect both the campus network design and the backbone network size and connection particular to the different architecture scenarios (see Section 4.5.1). Included in the diagrams is the identification of the key functional customer premise equipment required for communications.

In the node block diagrams, legacy equipment that supports Layer 3 networking protocols is directly interfaced to the campus network equipment. This type of user is also called a *standard user* as the

interface between the end system and the network utilizes a standard network protocol. It is envisioned that as new FAA systems come on-line, they will be specified to include standard user interfaces to the campus network. For those legacy systems which do not support Layer 3 networking protocols, either COTS or custom gateway equipment would be used to interface the user to the network, or a serial connection would be established between the legacy user and network equipment capable of encapsulating legacy data into Layer 3 packets (i.e. IP packets).

The equipment identifiers in the node block diagrams are intentionally generic. During the specification and detailed design of campus networks, equipment that meets the specific requirements of the FAA facilities and equipment at the nodes would dictate the specific equipment configuration required to implement networked communications. The detailed design and analysis of campus networks was beyond the scope of this study. In the architecture analyses included in Section 5, a set of specific commercial products that meet or exceed the node equipment requirements has been developed. The mapping of commercial products to the equipment identified in the node block diagrams can be found in Table 5.4-14.

A representative set of node diagrams for the Mansfield TRACON is provided in Figures 4.6-1 through 4.6-4. A separate diagram is provided for the baseline architecture, architecture Scenario 1A and 1B, and architecture Scenario 2. Block diagrams of all of the nodes in the representative architecture are provided in Appendix B. The following assumptions are applicable to the development of node diagrams:

- For various FAA end systems, raw data interfaces are assumed to be accessible.
- FAA circuits classified in TIMS as supporting ADVO and MISC services as well as a majority of the circuit carrying MNTC services currently connected to the PSTN are transitioned to an operational voice LAN providing a connection to the backbone network and PSTN; other MNTC circuits are transitioned to a direct connection to a local router for data encapsulation.
- FAA circuits classified as carrying ADVO, MISC or MNTC service and connecting a FAA facility to the PSTN are assumed to be a single phone line if the circuit monthly recurring charge (MRC) is less than \$125.
- FAA circuits classified as carrying ASOS service and connecting the Acquisition Control Unit to the PSTN are assumed to carry voice traffic. These circuits are transitioned to packet voice.
- TRACON, ARTCC, and AFSS circuits classified as carrying ADVO service and with associated MRC of \$125 to \$1,000 are assumed to be fractional T1 lines connecting to internal voice switches.
- SSU, CASFU, FSDO, and SMO facility circuits classified as carrying ADVO service and with MRC of \$125 to \$750 are assumed to support Centrex voice services.
- TIMS circuits with \$0 MRC or listed as “no accts” for a particular FAA facility were not included in the study.

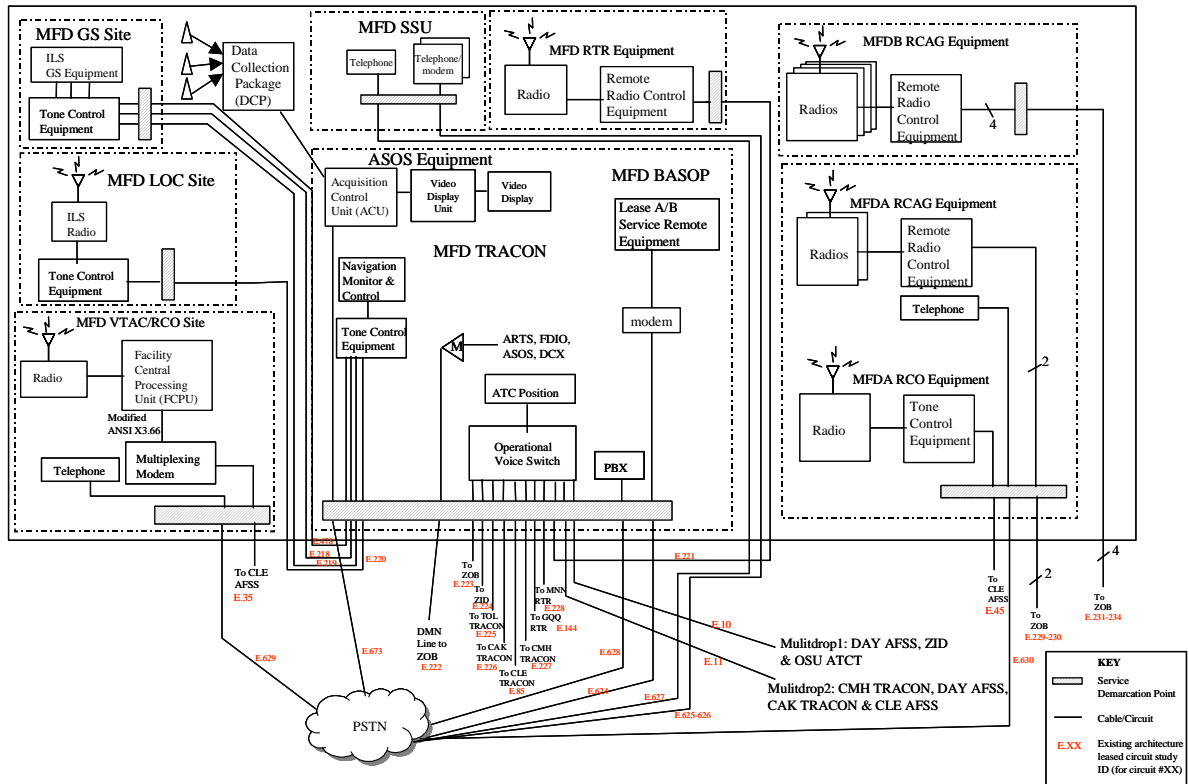


Figure 4.6-1: Mansfield TRACON Baseline

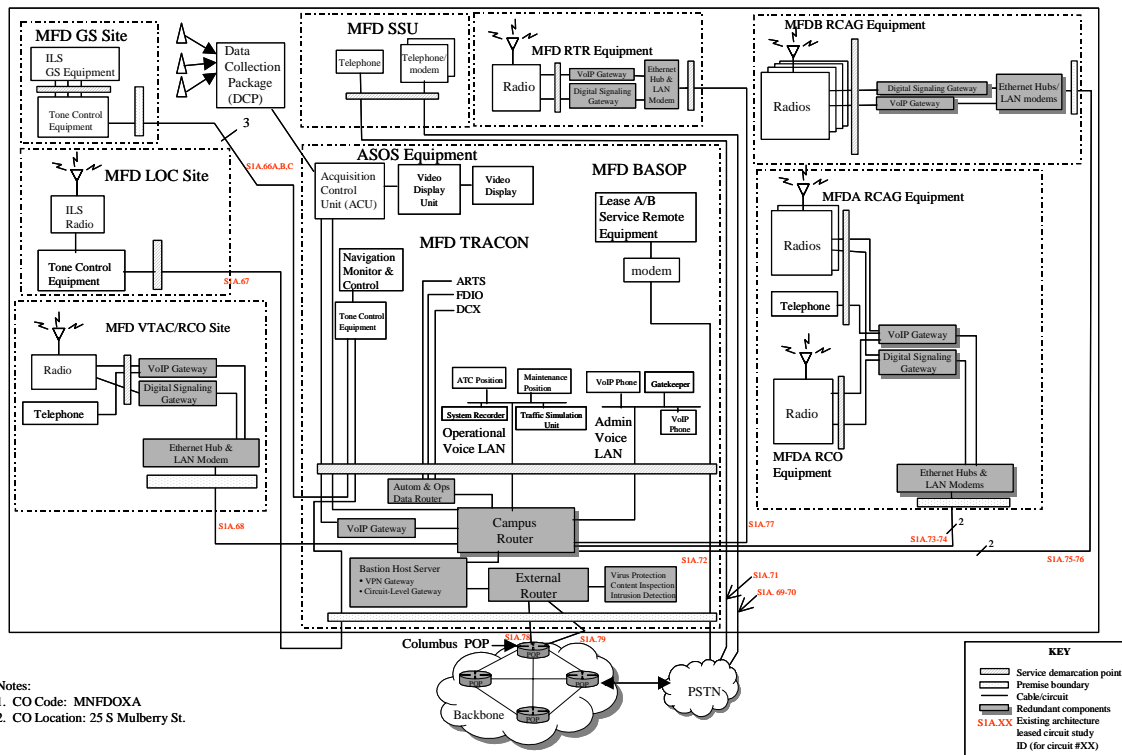
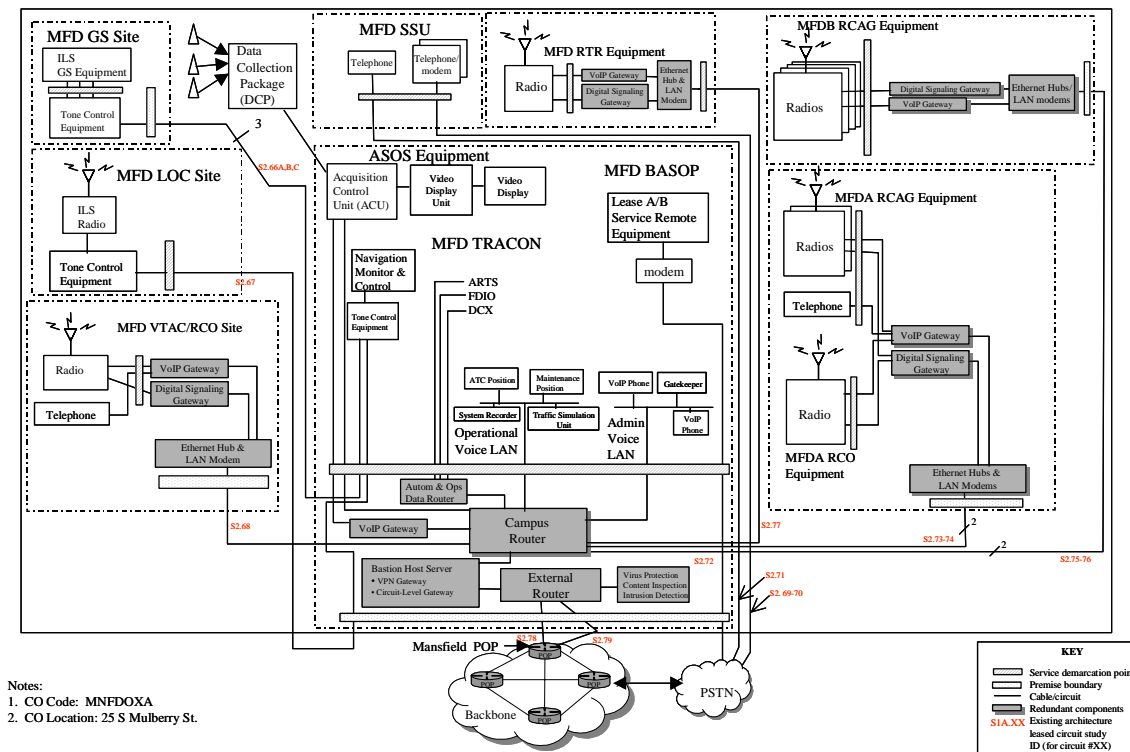
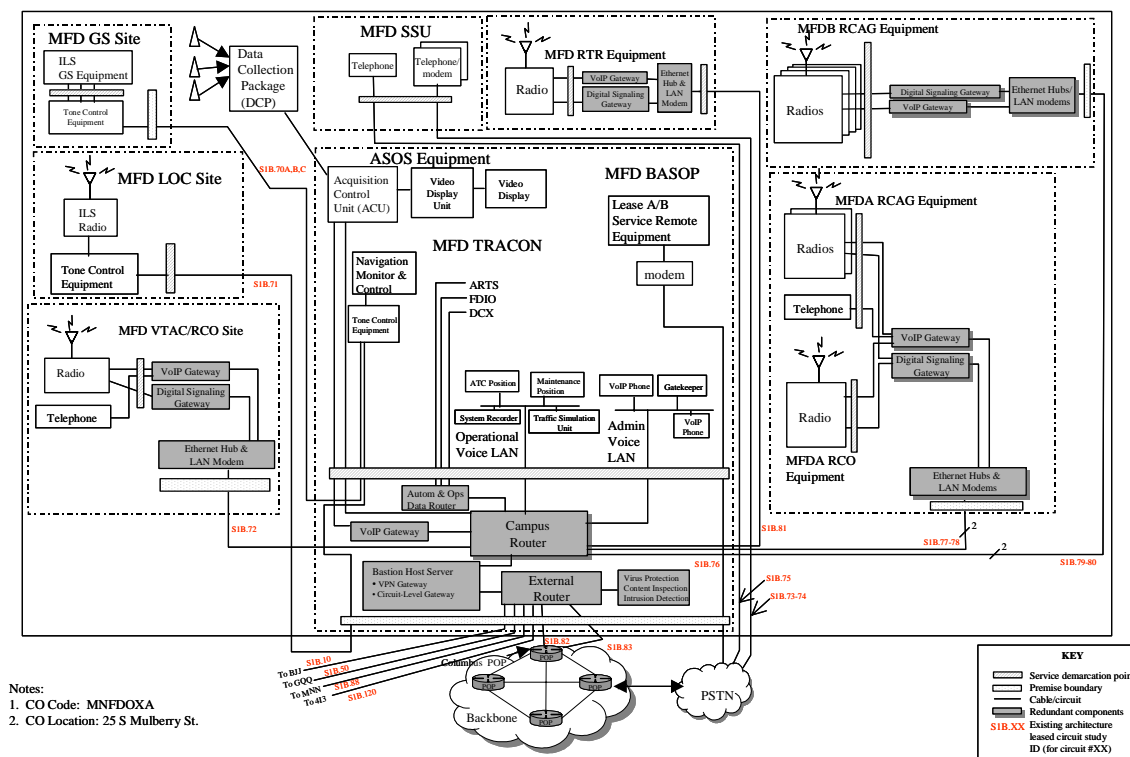


Figure 4.6-2: Mansfield TRACON Scenario 1A



The differences among the architectures can be seen upon close inspection of the figures above. Each of the proposed network architectures implements a campus area network at the Mansfield Lahm Municipal Airport and vicinity. In all proposed architecture scenarios, external connection to the commercial packet backbone network is made through a screened-subnet firewall.

In Scenario 1A, all external connections are to the Columbus, Ohio backbone access POP. For Scenario 1B, this connection is also present; however, there are also dedicated leased connections to small or remote FAA facilities in the vicinity of Mansfield. (See bottom of Figure 4.6-3). In this architecture, Mansfield acts as a regional hub for the small and remote nodes, providing the interface to the backbone network. Like Scenario 1A, all connections are made directly to the backbone network in Scenario 2. In this case, however, the network access POP is local, in Mansfield, Ohio (note the POP identifier in Figure 4.6-4).

4.6.2 Network Circuits

A list of network circuits was compiled for each of the representative architectures based on the connections required between campus network facilities and for external communications for network nodes. A list of circuits also was compiled for the baseline architecture scenario. Circuit numbers for each architecture are shown on each of the node block diagrams.

The baseline architecture includes nearly 900 individual leased communication circuits. Many are low bandwidth connections and have low utilization. The proposed network architectures each have a total of approximately 175 circuits. Many of these circuits are higher bandwidth connections as compared to the baseline scenario and can be sized to specific, measured data rate requirements. The proposed architectures represent nearly an 80% reduction in the number of circuits. Complete lists of circuits are provided in Appendix C for the baseline and proposed architectures.

5. EVALUATION OF THE ZOB ARCHITECTURE

5.1 TRANSITION ISSUES ASSOCIATED WITH ZOB ARCHITECTURE

This section provides an overview of the current voice communications equipment in use in the NAS. It then examines the architecture of the Voice Switching and Control Systems (VSCS) equipment in detail. A transition from the VSCS interface to the trunks, to a modern VoIP interface is provided, showing the intermediate steps for phasing in this technology and the resultant end state of such an approach.

Finally, issues and risks associated with this transitioning are explored.

5.1.1 Current NAS Voice Equipment and Interfaces

The FAA owns and leases a huge variety of equipment to maintain voice communications in the NAS. Equipment includes telephones, wiring, conference bridges, consoles, PBXs, and voice switches (VSs). Of these, the PBXs and voice switches are by far the most costly and complex items. This section will focus on this equipment.

The FAA maintains a large number of voice switches and proprietary PBXs. Figure 5.1-1 shows the major operational and administrative voice switches that are currently in use. This equipment is also tabulated in Table 5.1-1, and is briefly described in the following paragraphs. By far the most complex of this equipment is the Voice Switching and Control System (VSCS). Subsequent sections will detail the configuration and interfaces of the VSCS, so that the scope of the transition problem can be understood.

Operational Telephone System (OTS)

The OTS is located at the Air Traffic Control System Control Center (ATCSCC) in Herndon, VA and is used to conference participants for the daily air-traffic flow-control discussions. The OTS consists of a NEAC 2400 PBX plus other components (Conference Bridge, consoles, cabling) which are owned by the FAA. The responsible organization is AOP-400, OTS Program Manager.

ATCSCC Administrative Voice Switch

This is the Administrative VS at the ATCSCC.

Voice Telecommunications System (VTS)

The VTS is an administrative VS used at Regional Offices (ROs), ARTCCs, TRACONS, the ATCSCC, and other FAA locations. The VSs are Northern Telecom Meridian I, option 61, 71, or 81 PABXs. They usually have a conference bridge installed. The VTSs are used in the Electronic Tandem Network (ETN) and Emergency Voice Communications System (EVCS). Dyn Corp maintains the VTS.

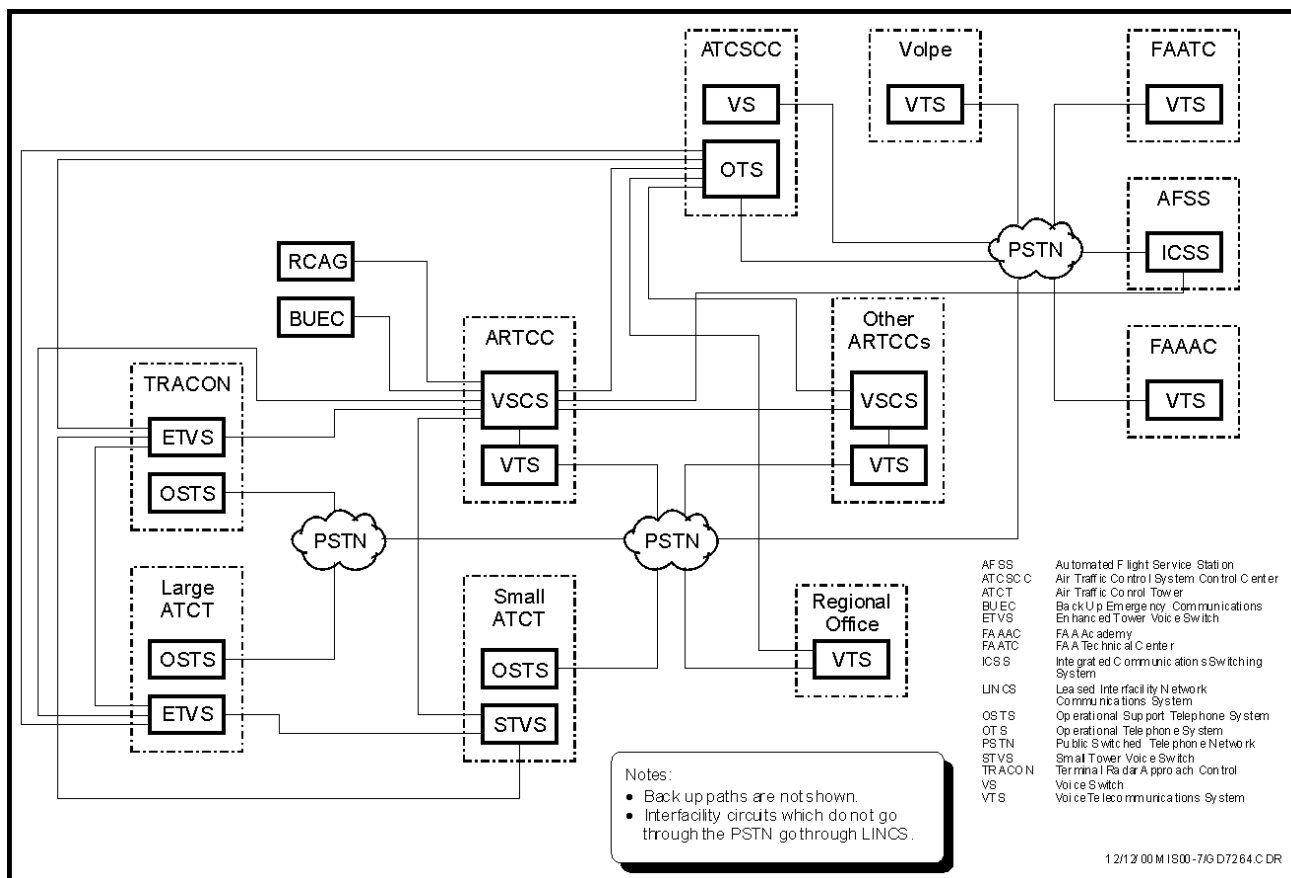


Figure 5.1-1: Overview of the NAS Showing Legacy Voice Switches⁶²

Table 5.1-1: Major Voice Switching Equipment Currently in Use in the NAS

Switch Type*	Facilities*	Major Use
ATCSCC VS	ATCSCC	Administrative Voice
OSTS	ATCTs and TRACONS	Administrative Voice
VTS	Regional Offices (ROs), ARTCCs, TRACONS, ATCSCC	Administrative Voice
ICSS	AFSS	Operational Voice (Flight Service Specialists for Pilot Briefings)
ETVS	ATCTs and TRACONS	Operational Voice
OTVS	ATCSCC	Operational Voice (Conferencing for Air Traffic Flow Discussions)
STVS	Air Traffic Control Facilities with less than 4 positions	Operational Voice
VSCS	ARTCCs	Operational Voice

* Note: See Figure 5.1-1 above for acronym definitions

Small Tower Voice Switch (STVS)

The STVS is used at Air Traffic Control Facilities with less than 4 positions. The STVS is an integrated air-ground and ground-ground voice switching system manufactured by Denro. The STVS is designed for low activity operations and accommodates up to four operator positions. STVS systems may be

linked to fulfill larger requirements. The STVS is a joint FAA/Department of Defense (DOD) project. Two hundred and forty systems have been delivered and commissioned.

Enhanced Terminal Voice Switch (ETVS)

The responsible organization for the ETVS is AND-320, Voice Switching/Recording Team. On June 8th, 1999, an In Service Review was held for ETVS at which the Director, Airway Facilities Service, approved the system for deployment. ETVS replaces analog voice switching systems in air traffic control towers and TRACONS, providing a reliable telecommunications system that keeps pace with rapid advances in technology.

5.1.2 VSCS

The VSCS is a voice communication system (based on the Harris 20-20 switching system) that is in operation at ARTCCs in the continental United States and Alaska. The VSCS provides air traffic controllers at ARTCCs with air-to-ground (A/G) and ground-to-ground (G/G) voice communication capability. VSCS interfaces with radio control equipment and ARTCC voice legal recorders. AOS-520 is the branch in AOS that provides site support for VSCS.

The VSCS System Architecture is presented in Figure 5.1-2. ATC operator positions are connected via the switching subsystem to other ATC operators, the PABX tie lines, Interfacility trunks, BUEC radios, and the Very High Frequency (VHF)/Ultra High Frequency (UHF) radios. Other functions are provided for control, maintenance, and testing, but this is the basic requirement of the system.

5.1.2.1 VSCS Signaling Interfaces

Figure 5.1-3 presents a simplified view of the VSCS. ATC operators at the common console have their communications switched through either the A/G switch assembly or the G/G switch assembly. The VSCS trunk interface block, shown in Figure 5.1-3, is expanded in Figure 5.1-4. In Figure 5.1-4, the block marked MDS is the Master Demarcation System.

The MDS is the Service Delivery Point (SDP) for analog services in the ARTCCs and some of the Large TRACONS. The MDS is located in the Control Wing Basement of the ARTCCs and is the termination point for leased analog telecommunications. The MDS also terminates the Radio Communications Links (RCL), Low Density Radio Communications Link (LDRCL), and FAA Telecommunications Satellite (FAATSAT) telecommunications assets. The MDS interfaces with the Automated Line Test Equipment, which uses Dual-Tone Multifrequency (DTMF) signaling to access responders located at remote sites. The MDS employs a 110-block type interface. In addition to the analog services, high-speed data circuits are terminated on a digital Demarcation in the MDS⁶³.

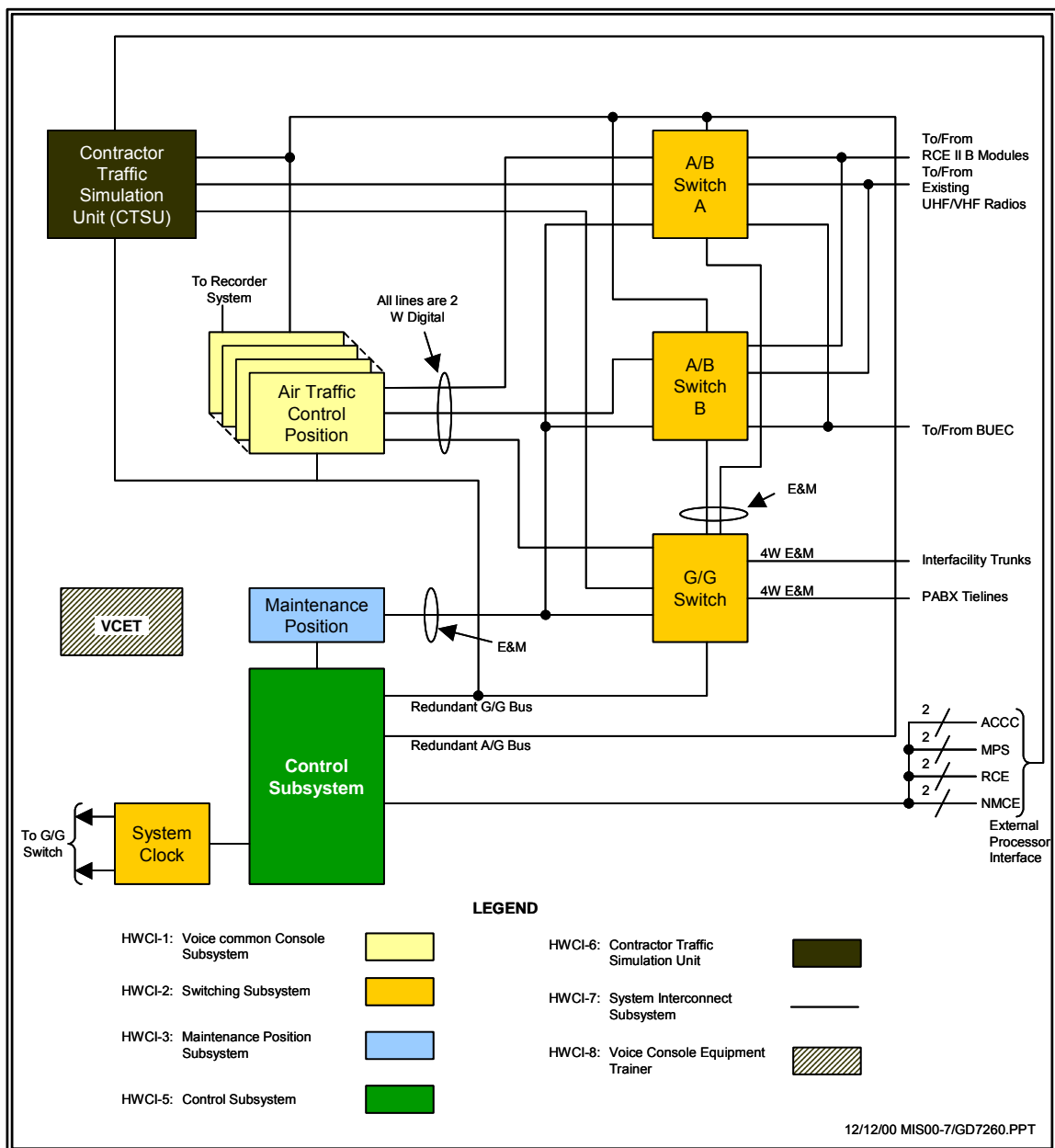


Figure 5.1-2: VSCS System Architecture ⁶⁴

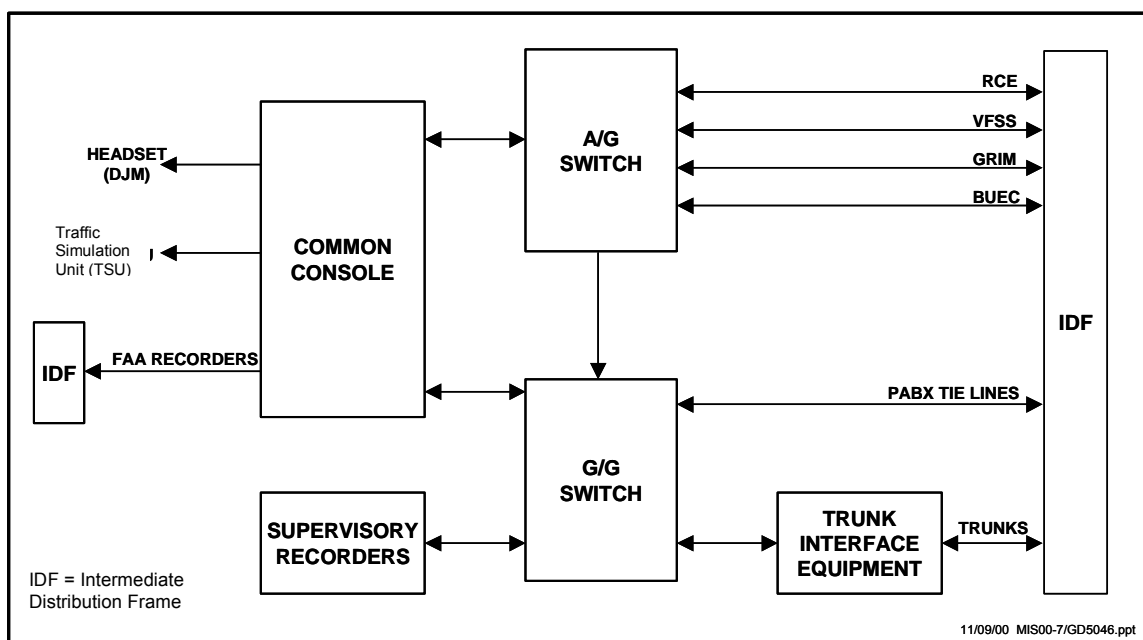


Figure 5.1-3: Simplified VSCS Interface Diagram⁶⁵

From Figure 5.1-4, it is clear that the VSCS supports a large number of signaling interfaces. Many of these interfaces are a legacy of pre-divestiture of the Bell System. Prior to divestiture of the Bell System, the signaling and supervision needed to operate the various interphone circuits were mostly under the purview of the serving company, usually the local exchange carrier. Interphone circuits, and some radio circuits, as originally provisioned by the telcos, utilized signaling and supervision equipment that often was contained in the central office, or in the provider's equipment that was located at the customer premise, or some combination of the above. Many of the *key systems* (small telecommunications switches with a panel of buttons at the controller positions) were designed to rely on central office-provided signaling and the availability of 2-wire circuits.

When the Leased Interfacility NAS Communications System (LINCS) program was launched, it was recognized that if circuits were to be patchable or switchable between Telco and RCL, for example, it would be necessary to imbed the signaling and supervision in the FAA Customer Premises Equipment (CPE), or end user equipment. In addition, signal levels would need to be compatible so the LINCS program standardized on a) the zero-loss circuit, and b) no signaling to be provided by the network. These provisions were included in the LINCS contract. However, several new ATC voice switch procurement programs that were in the pipeline went to the manufacturer with the same technical specifications that had been used over the years when the Telco industry provided the special treatment equipment.⁶⁶ For example, the VSCS product specification cites that the VSCS will provide:

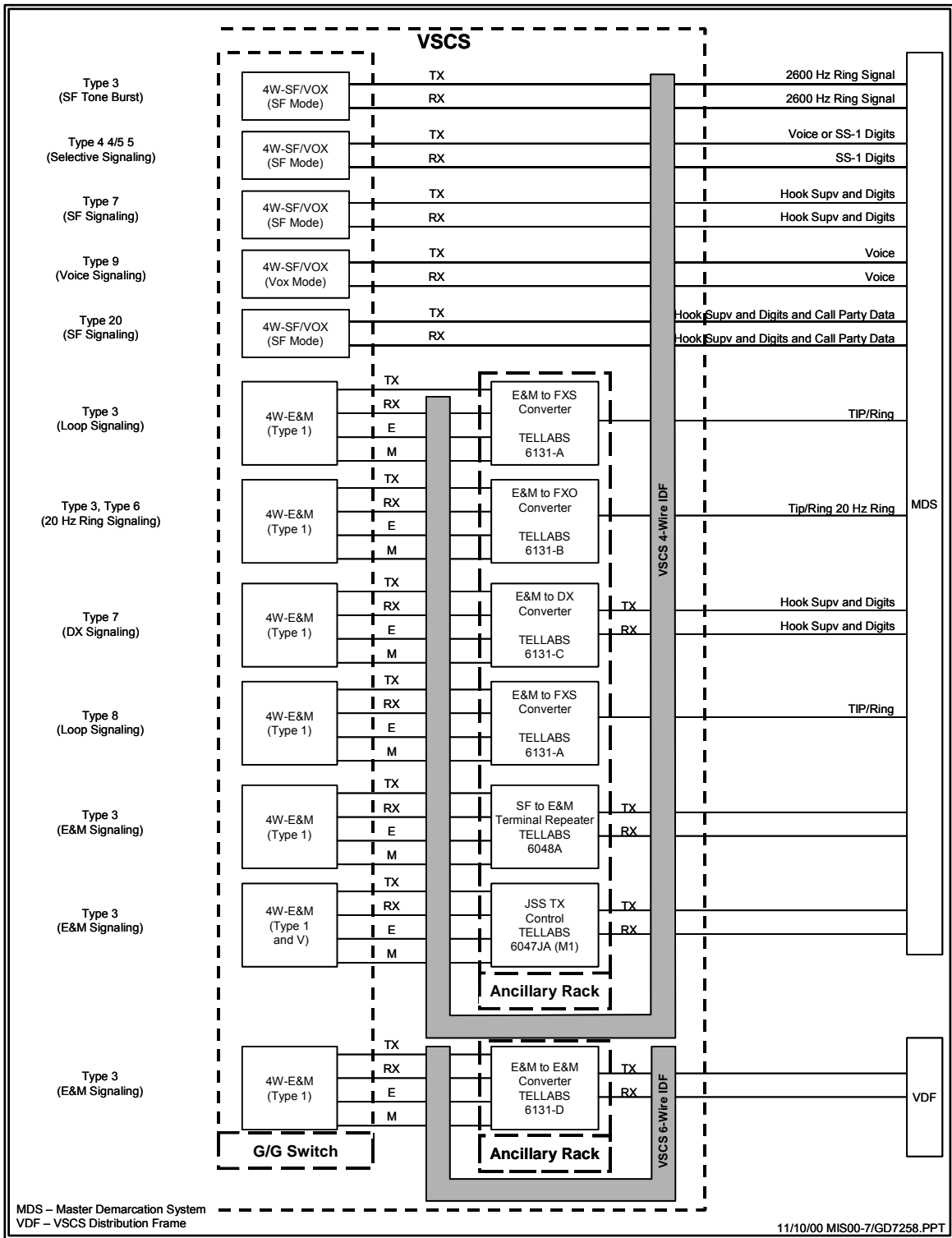


Figure 5.1-4: VSCS Trunk Interface Summary⁶⁷

3.5.2.2.3.2 Trunk Signaling Interfaces with Existing Systems – The trunk interface, as specified in the VSCS-Trunks IRD, when appropriately class marked and equipped with appropriate equipment, shall be capable of interfacing with the older analog systems including WECCO 300⁶⁸.

Table 5.1-2 shows the types and signaling characteristics of the existing FAA interfacility trunks. From Table 5.1-2 and Figure 5.1-4 it is clear that transitioning the ARTCC to ARTCC/TRACON/ATCT Interphone service is a complicated task. Additionally, the radio circuits also have special requirements. In addition to the voice information, radio control signals must be transmitted across these circuits. The ATC can send a push-to-talk control signal and switch the radios from main to standby, using specialized control equipment that provide a data above voice (DAV) function. This is provided by special modems, called Radio Control Equipment (RCE), at both the ARTCC and the RCAGs. Finally, the VSCS interfaces to the PABX, which has a proprietary interface.

5.1.2.2 Functionality Provided by the VSCS

The VSCS is a computer-controlled switching system that provides air traffic controllers with the means to establish all voice circuits necessary for ATC operations. Up to 430 positions can be served by the VSCS. ATC personnel use the VSCS for:

- A/G radio: Controllers use the VSCS to access and provide proper control of the remote UHF and VHF A/G transmitters and receivers through which they communicate with pilots. The VSCS ensures that incoming A/G communications from pilots are routed to the proper control position. The VSCS also provides connectivity to the BUEC radios.
- Intercom: Through the VSCS, ATC personnel have access to other control positions within the same facility (ARTCC).
- Interphone: Through the VSCS, ATC personnel have access to other controllers located within another ATC facility.
- External Circuits: The VSCS provides access to the Public Switched Telephone Network (PSTN), and Federal Telecommunications System (FTS) and local telephone exchanges via an interface with the PABX in the facility⁶⁹.

The VSCS, in conjunction with the common console, allows the ATC position the ability to perform a variety of control and communications functions. The ATC operator can perform the following control functions:

- G/G Non-override Voice Routing
- G/G Override Voice Routing
- Call Forwarding
- Holler On/Off
- Position Relief

Table 5.1-2: Existing FAA Trunk Types for ARTCC

FAA Trunk Circuit No.	Trunk Description	Trunk Audio Line	Signaling Outbound	Signaling Inbound
Type 3	Used for point-to-point communication between the facility and distant locations	2-wire or 2-wire	<ul style="list-style-type: none"> • Automatic with manual re-ring by means of the R&F key • Voice call signaling • 20 Hz ring 	<ul style="list-style-type: none"> • DA termination • Signaling dependent on remote equipment • Side tone from Telco
Type 4	Used for multi-point communication	4-wire	<ul style="list-style-type: none"> • Voice call signaling 	<ul style="list-style-type: none"> • SS-1 selective signaling • Voice call signaling • Side tone from Telco
Type 5	Used for multi-point communication	4-wire	<ul style="list-style-type: none"> • SS-1 selective signaling, or 2400/2600 FSK 	<ul style="list-style-type: none"> • SS-1 selective signaling, or 2400/2600 FSK • Side tone from Telco
Type 4/5	Used for multi-point communication	4-wire	<ul style="list-style-type: none"> • Voice-call or selective signaling 	<ul style="list-style-type: none"> • SS-1 selective signaling • Side tone from Telco
Type 6	Dedicated point-to-point; used to connect to central office (CO) lines and station lines from adjacent PBXs	2-wire	<ul style="list-style-type: none"> • Loop start • Dual out using DTMF or 10 pps 	<ul style="list-style-type: none"> • 20 Hz ringdown
Type 7	Dedicated point-to-point; PBX tie trunks (used between Interphone Switching System and dial-type PBXs)	4-wire	<ul style="list-style-type: none"> • Dial out using DTMF or 10 pps 	<ul style="list-style-type: none"> • Loop start • Dial in using DTMF or 10 pps • Side tone from Telco
Type 8	Dedicated point-to-point; 2-way or 1-way incoming to/from local vicinity points	2-wire	<ul style="list-style-type: none"> • Automatic ringdown • Manual ringdown • Voice signaling 	<ul style="list-style-type: none"> • Loop start • Ring down • Dial in using DTMF or 10 pps • Side tone GFE
Type 9	"Hot line" optionally available for high priority communication between certain ARTCC positions and designated positions in terminal or tower	4-wire	<ul style="list-style-type: none"> • Voice-call signaling 	<ul style="list-style-type: none"> • Voice call signaling • Side tone from Telco
A/G trunk	Dedicated point-to-point to RCAG site	4-wire	<ul style="list-style-type: none"> • In band tones 150 bps; FSK and/or AM dependent on the control equipment interfaced 	<ul style="list-style-type: none"> • In band tones 150 bps; FSK and/or AM dependent on the control equipment interfaced

- Voice Monitor

The communications functions include:

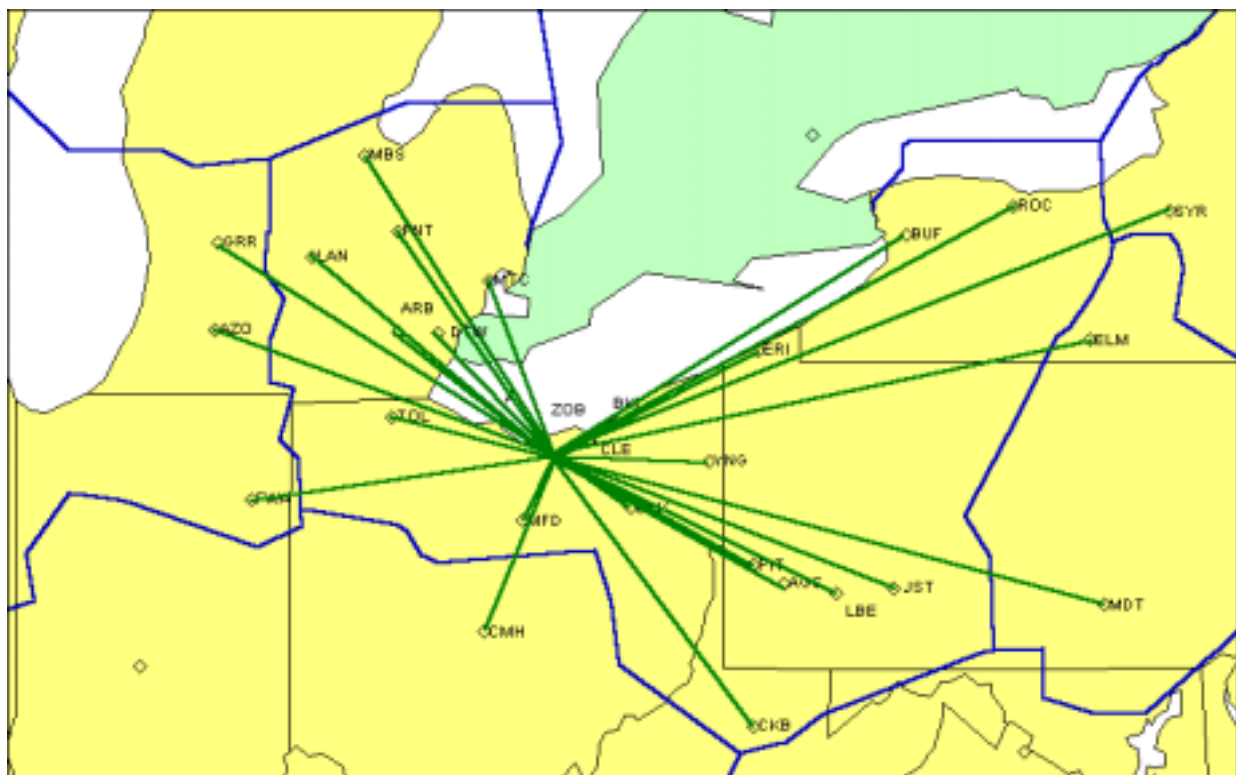
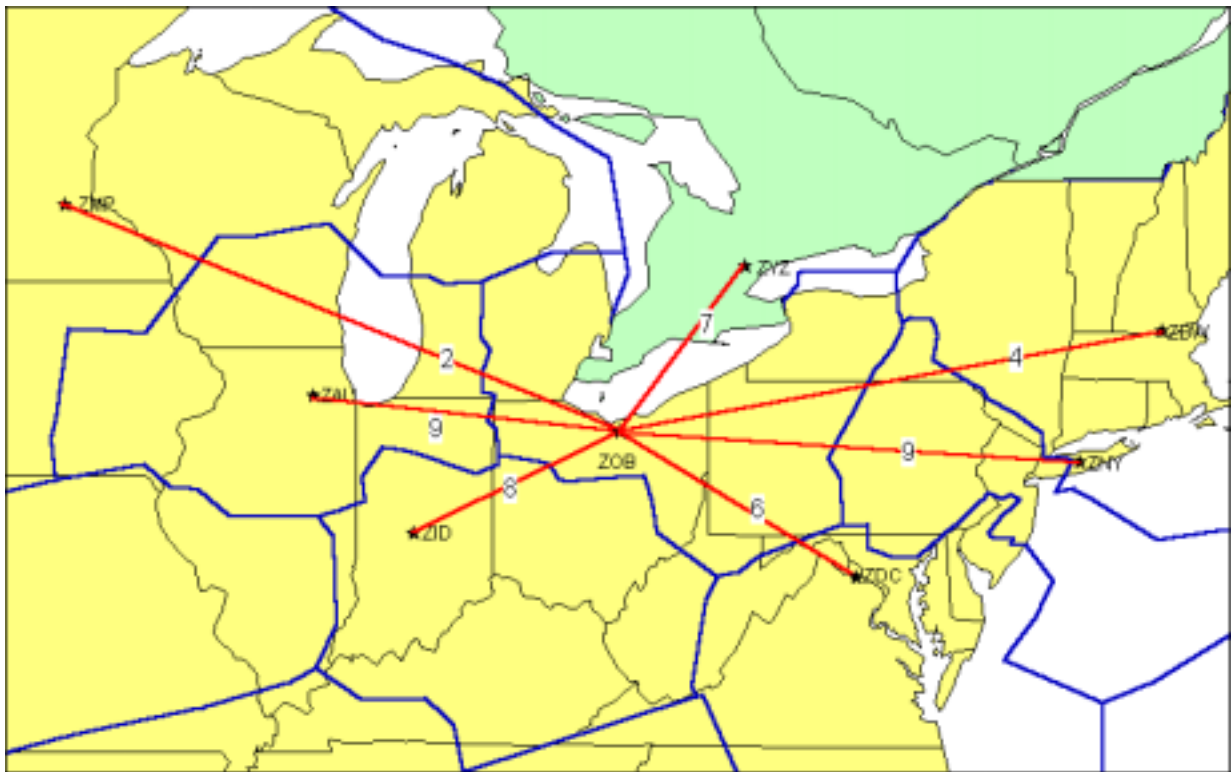
- Originate Override Call
- Originate Intercom Calls
- Originate Interphone Calls
- Originate Private Automatic Branch Exchange Calls
- Originate Meet-Me Conference Calls
- Originate Preset Conference Call
- Originate Progressive Call
- Call Join
- Call Hold
- Call Release

5.2 INTEGRATION/TRANSITION TO VOIP

From Section 5.1, it should be clear that the transition from analog voice to VoIP for operational voice circuits is a very complex undertaking. In Figure 5.1-1, the VSCS is shown to interconnect to virtually every operational voice switch type in use in the NAS. The VSCS must interconnect with:

- Other VSCSs
- ETVS
- STVS
- ICSS
- OTS
- PSTN
- RCE equipment
- BUEC equipment

To provide specific detail of the VSCS provided connectivity, several figures from an earlier report are reproduced here. Figure 5.2-1 shows the ZOB ARTCC to ARTCC Interphone Connectivity. From the figure, we see that the VSCS at ZOB must interface to the VSCS equipment at the six adjacent ARTCCs, as well as to the switching equipment at ZYZ (Lester B. Pearson International ACC, located in Toronto, Ont.). Figure 5.2-2 shows that the VSCS at ZOB also interfaces with 27 other ATC facilities in the regions, including TRACONS, ATCT, and AFSS. Figure 5.2-3 shows the large number of RCAGs and BUECs that interface to the ZOB VSCS.



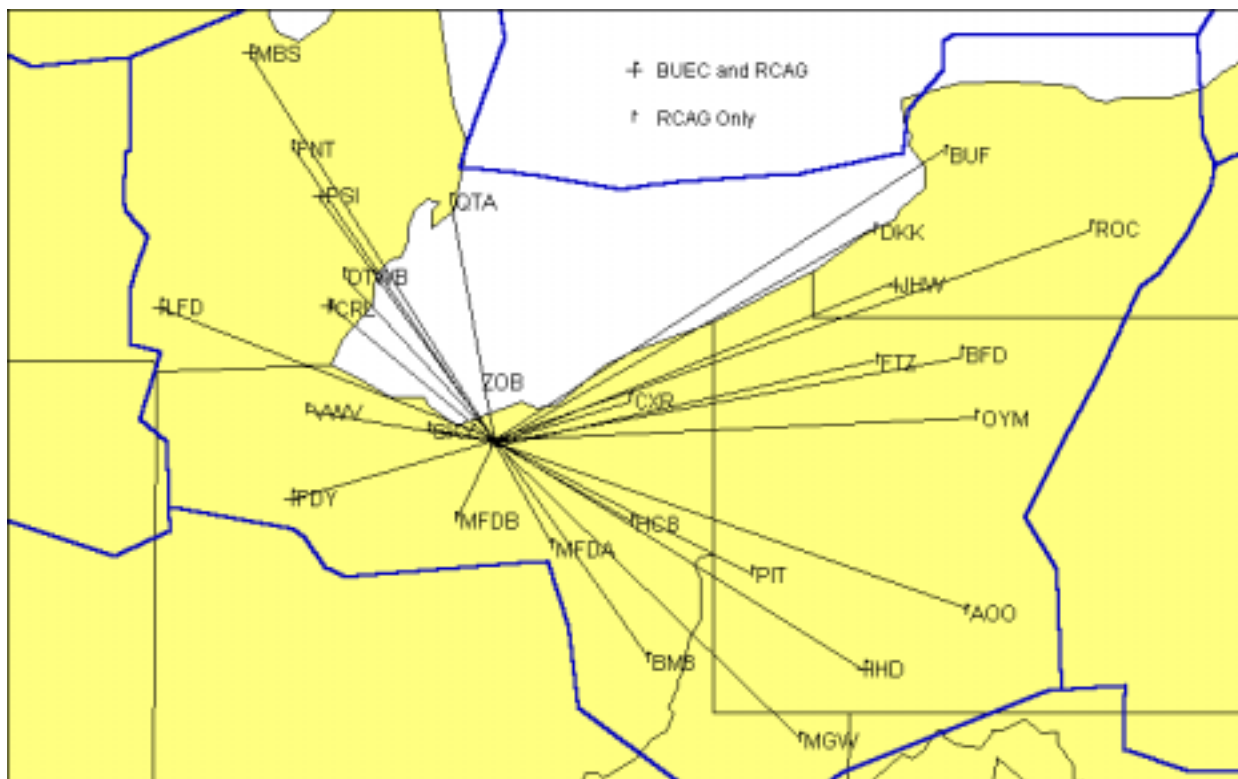


Figure 5.2-3: RCAG and BUEC Connectivity to ZOB⁷²

To support the legacy trunk interfaces, the VSCS must support all of the signaling types that are enumerated in Table 5.1-2, mostly through the use of a set of Tellabs converters, as depicted in Figure 5.1-4.

Additionally, this equipment provides the ATC operator the functions that are enumerated in Section 5.1.2.2. It does all of this with a specified system level availability of 0.9999999⁷³. The position-level availability requirements are shown in Table 5.2-1.

Table 5.2-1: VSCS Position-Level Availability Requirements

Function	Required Availability
Radio A/G	0.9999
Intercom	0.9995
Interphone	0.9995

Any successful transition will probably require redundant hardware at pairs of facilities, so that circuits can be cut over incrementally. The following section gives a high level overview of the requirements of these transition states.

5.2.1 Transition States

Figure 5.2-4 presents a notional transition architecture for the VSCS. In this architecture, G/G and A/G voice circuits are dual analog/VoIP circuits. The VoIP gateway translates the analog voice and signaling for transmission over the managed packet network. The VSCS console equipment remains unaffected.

To understand the concept of Figure 5.2-4, refer back to Figure 5.1-3 and Figure 5.1-4. In Figure 5.1-3, we see that the common console is the interface for the ATC operator. All ATC operator actions and interfaces are unaffected by the architecture shown in Figure 5.2-4, since the interface between the common console and the A/G, G/G switches remains unchanged. From Figure 5.1-4, we see that the G/G switch has a 4-wire E&M interface to the Intermediate Distribution Frame (IDF). The IDF is a large relay rack on which are mounted 66-blocks (a type of telephone wire connector block), wire wrap panels and trunk patches.

Also note in Figure 5.1-4 that the multitude of signaling protocols currently in use is supported by the VSCS. Currently, Tellabs converters use the 4-wire E&M interface at the IDF to the required signaling protocol to support legacy equipment. As the NAS is transitioned to a packet-switched network, and specifically, as the VSCS is transitioned to VoIP technology, it is expected that these legacy signaling protocols will be eliminated. This will be accomplished because circuits are being retrofitted at both ends, in a pair wise fashion, gradually eliminating all legacy equipment. The functionality of the signaling protocols (not the protocols – just features of the protocols that must be maintained, such as voice call signaling) can easily be duplicated in the software functions of the more modern telecommunications software.

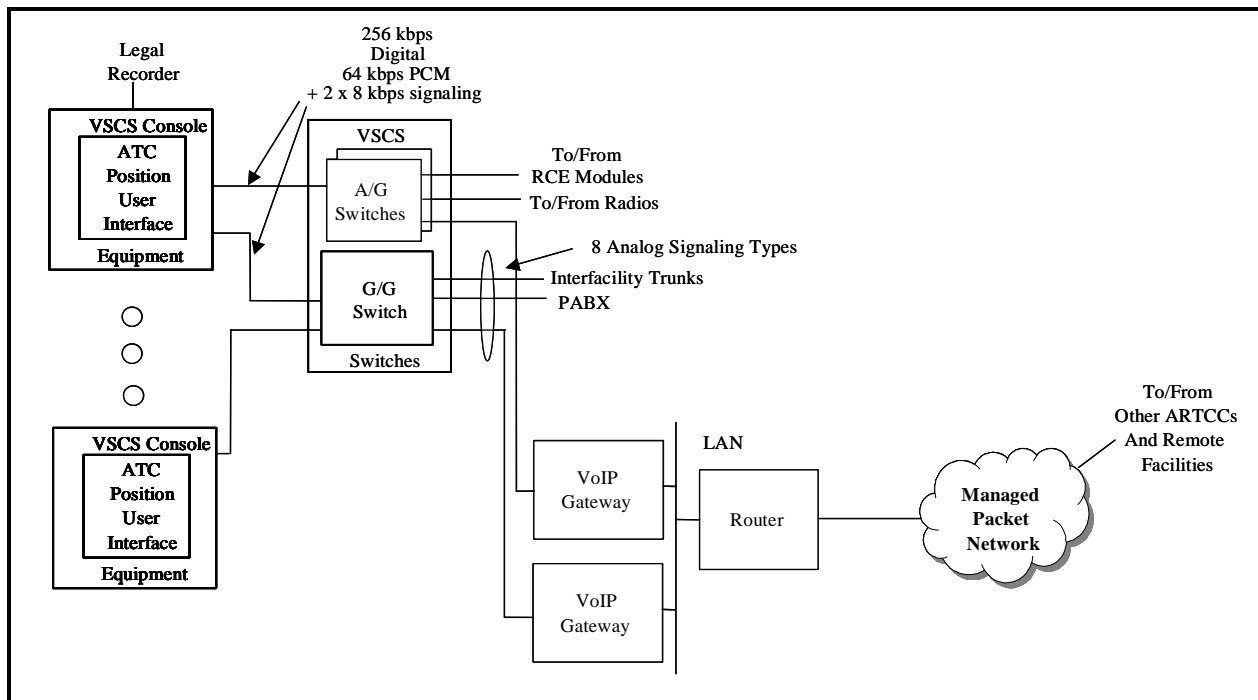


Figure 5.2-4: Notional ARTCC Transition Architecture

Most vendors of VoIP products make VoIP gateways that support the 4-W E&M interface. As an example, the CISCO 3600 router can be configured as a VoIP gateway. When so configured it can support either 2-wire or 4-wire E&M interfaces. The Cisco 3600 provides the following features⁷⁴:

The Cisco 3600 currently provides analog voice ports for its implementation of Voice over IP. The type of signaling associated with these analog voice ports depend on the interface module installed into the device. The Cisco 3600 series router supports either a two-port or four-port voice network module (VNM); VNMs can hold either two or four voice interface cards (VICs).

Each VIC is specific to a particular signaling type; therefore, VICs determine the type of signaling for the voice ports on that particular VNM. This means that even though VNMs can hold multiple VICs, each VIC on a VNM must conform to the same signaling type.

Voice ports on the Cisco 3600 series support three basic voice signaling types:

FXO---Foreign Exchange Office interface. The FXO interface is an RJ-11 connector that allows a connection to be directed at the PSTN's central office (or to a standard PBX interface, if the local telecommunications authority permits). This interface is of value for off-premise extension applications.

FXS---The Foreign Exchange Station interface. This interface is an RJ-11 connector that allows connection for basic telephone equipment, keysets, PBXs, and supplies ring, voltage, and dial tone.

E&M---The "Ear and Mouth" interface (or "RecEive and TransMit") interface. This interface is an RJ-48 connector that allows connection for PBX trunk lines (tie lines). It is a signaling technique for two-wire and four-wire telephone and trunk interfaces.

A Cisco 3660 router holds up to six network modules providing a maximum of 24 analog voice ports. Properly configured, this is roughly a \$37,000 router. Two routers are shown in Figure 5.2-4 to show a redundancy function, in order to get the required availability. Cisco provides a protocol for managing redundant routers in precisely this configuration. Hence, a rough order of magnitude, non-recurring cost for transitioning the trunks is \$100,000 for every 24 trunks.

5.2.2 End State

Before presenting a possible end-state configuration, some more insight into the construction of the VSCS is required. Refer to Figure 5.2-5. In Figure 5.2-5, we see that the common console interfaces to the VSCS Electronic Module, and then to the G/G and A/G switch assemblies. The VSCS Electronic Module is part of the VSCS common console equipment, and provides interfaces to the FAA Traffic Simulation Unit (TSU), the legal recording system, and facility power. The VSCS Electronic Module contains a

switch card that provides the interface to the switching subsystem. The interface is a digital subscriber line interface. The card provides two 8 kbps signaling channels and one 64 kbps μ -law pulse code modulation (PCM) voice channel. This is the obvious interface that any replacement Voice System should be compatible with. The situation becomes difficult when trying to convert the data channels into usable routing information.

Figure 5.2-6 presents a notional end state architecture for the ARTCCs. In this architecture, G/G and A/G analog voice circuits have been totally replaced with VoIP circuits. The analog G/G and A/G VSCS switch equipment remains, and provides a means to convert all signaling to a common type (4 wire E&M). The common console remains, so that the ATC user interface remains unchanged. Despite a complete change in the underlying technology, ATC operations remain completely unaffected.

Note that this is but one alternative of many for transitioning to VoIP technology. In this alternative, the VSCS remains virtually intact. While this might be perceived as a disadvantage to this particular architecture, the approach does have several advantages. Some advantages to this approach are:

- The ATC user interface remains unaffected.
- All signaling types are gradually moved to one common signaling standard, removing the proliferation of signaling standards from the NAS. Special functionality that was implemented in hardware is now performed in the software instructions in the routers.
- Voice compression allows an immediate savings in MRC of leased lines. Furthermore, since routers support both real time and historic views of line utilization, intelligent provisioning of line capacity can be accomplished, once true capacity requirements are documented.
- The transition and end states are complementary. Furthermore, when it becomes time to replace the common console equipment, the routers provide a standardized interface that can also perform the switching function, obviating the need for the VSCS.

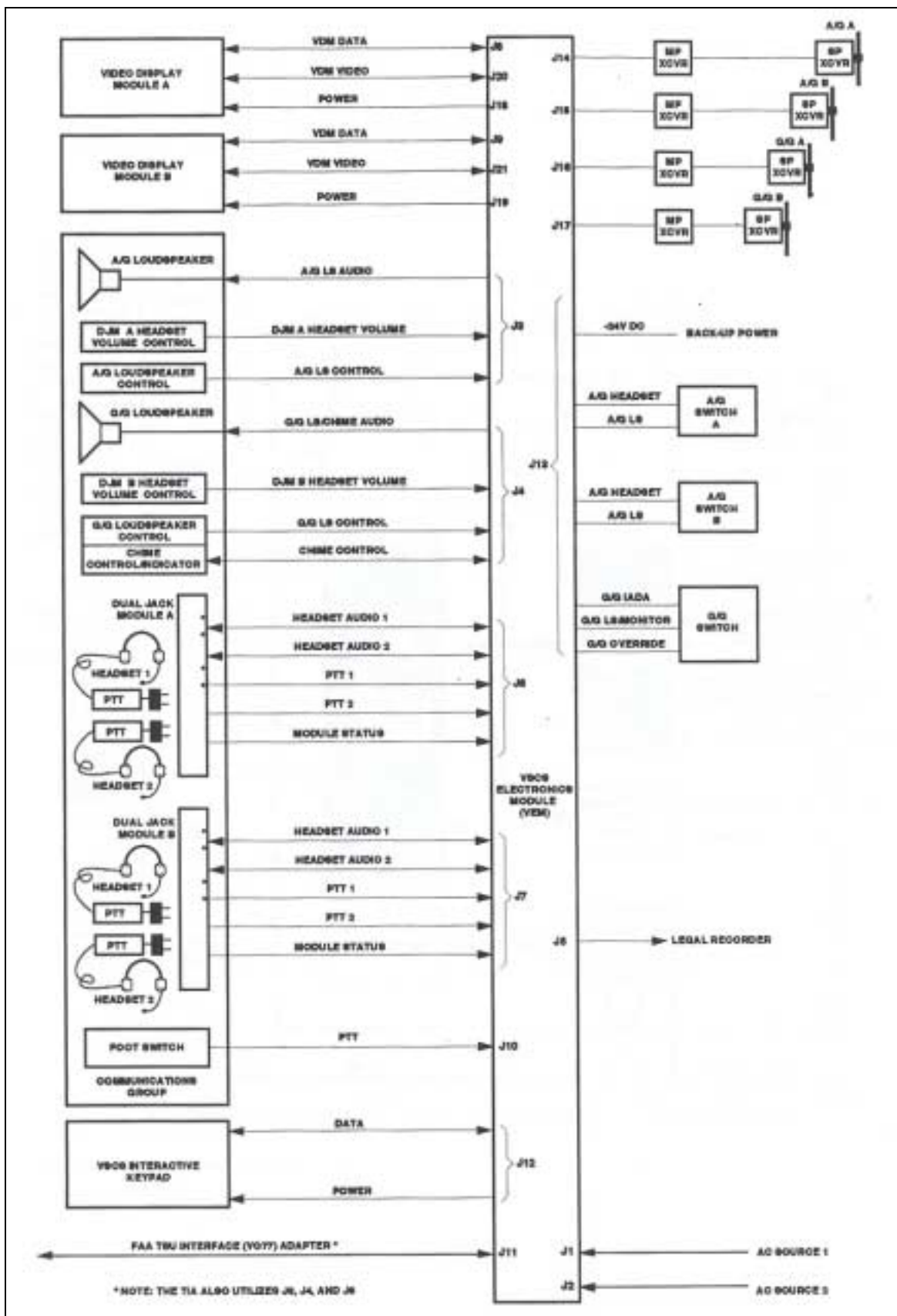


Figure 5.2-5: VSCS Console Equipment Interface Diagram

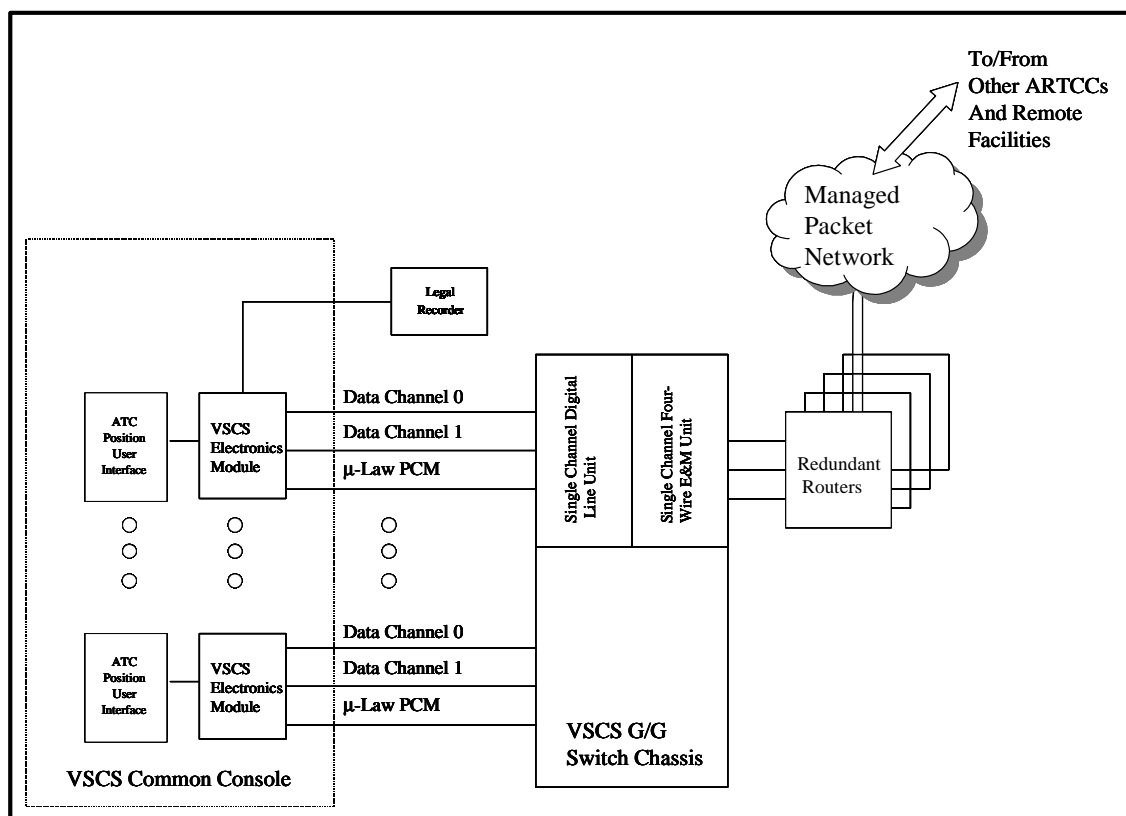


Figure 5.2-6: Notional ARTCC End State Architecture

5.2.3 Transition Issues/Problems

Remote Facilities. RCAGs and BUECs are remote facilities. These facilities can present unique resource and space limitations. Some of these facilities require government escort for site access. This includes access required for site surveys, site preparation, circuit terminations, equipment installation, or circuit testing. While some sites are equipped with a separate telephone room, others only have an outside box (roughly 3 feet by 4 feet) for telecommunication services. Space should not be a problem at sites that have a separate telephone room, but will likely be a problem at sites equipped with outside boxes⁷⁵.

Due to escort requirements at many remote sites, as well as the difficulty of reaching some of these sites, a transition strategy that minimizes trips to the remote sites is probably required. In other words, a transition plan requiring separate visits for a survey, site preparation, site installation, and cutover would be very difficult to implement based on the availability of FAA resources.

Funding Profile. The cost of establishing redundant switching structures throughout the NAS could be quite high. The analog circuits can only be cut over incrementally as each additional facility has the redundant switching structures installed. Hence, the savings on recurring costs (leased telecommunications assets) may not initially offset the cost of installing the parallel infrastructure, causing a hump in the costing profile. All transition activities and plans must be accomplished within the

scope of the approved FTI financial baseline. Facilities and Equipment (F&E) funding would be used for non-recurring costs associated with establishing the FTI infrastructure (e.g., installing the redundant switching structures).

Limitations imposed by the complexity and unique functionality of the VSCS. Controllers interact with the VSCS through the common console. The functionality that the VSCS provides correlates to a learned set of operator actions on the part of the Air Traffic Controllers. Changes in these operator actions must be minimized to ensure a successful transition to any new technology. These operator actions are initiated through a touch screen at the common console. As an example, if an ATC operator wishes to originate an override call:

Touch idle latching override DA button for desired override (OVR) call connection

OR

*Touch and hold idle non-latching OVR DA button for desired override call connection.
(Touch button continuously while communicating.)*

Any new equipment should be able to interface to the common console and provide the override functionality with the same sequence of operator actions that was described above. The OVR functions are an inherent part of the current switch configuration and trunk types. The user-to-network interface used in the end state must translate that information to the router in a format that will produce the desired outcome (e.g., equivalent functionality). Other unique characteristics of the VSCS that will lend to a difficult transition include the high overall availability of the system (0.9999999) and the large number of signaling protocols that are supported. In some cases, these signaling protocols can be eliminated, as the evolution of equipment at all circuit ends obviates the need for some of the older signaling types. However, some of the signaling formats provide special capabilities, such as the type 9 “hot line” signaling, which is also referred to as the “holler line”. This functionality will have to be replicated to ensure a successful transition.

5.3 PERFORMANCE ASSESSMENT

For this task several assessments were performed to gauge the performance of the proposed communication network architectures (reference Section 4.5.1) compared to baseline communications performance for the representative set of ZOB facilities. These included latency analysis, availability analysis and cost analysis. These analyses are addressed in the following subsections.

5.3.1 Latency

Section 4.4.3.2 addresses the difficulties in identifying latency goals and requirements specific to FAA communications as well as for end-to-end systems. Based on guidance provided in several FAA requirement documents, a set of latency constraints for general categories of voice and data were defined

for use in this study. These latency values for communications are provided in Table 4.4-4 and summarized as follows:

- Critical Data Communications: 300 ms
- Essential/Routine Data: 600 ms
- Operational Voice: 150 – 250 ms (the 250 ms value includes some allocation to end-systems)
- Administrative Voice: 300 ms

Of the latency constraints in the list above, the most stringent values apply to critical data (i.e. short-range and long-range radar data) and critical operational voice communications (i.e. air-ground communication).

Due to the large number of circuits included in the representative architecture, a subset of communication links were selected for analysis. These links were selected as representative cases of the communications with the most stringent latency constraints. A list of the representative cases and associated specific circuits used for analysis are provided in Table 5.3-1.

Table 5.3-1: Latency Analysis Scenarios

Representative Scenario for Latency Analysis	Representative Architecture Circuit
Terminal critical air-ground voice (TRACON to RTR)	Mansfield (MFD) TRACON to Marion (MNN) RTR
En route critical air-ground voice (ARTCC to BUEC/RCAG)	ZOB ARTC to Flint (FNT)
Terminal to En Route critical A/G voice (TRACON to ARTCC)	Cleveland (CLE) TRACON to ZOB ARTCC
En Route radar data (ARSR to ARTCC)	QDT ARSR to ZOB

For each representative circuit, a latency block diagram was developed based on the Scenario 1A and Scenario 2 architectures.⁷⁶ The latency block diagrams for the representative circuits includes those communications functions and equipment which influence latency. This includes a wide area network which comprises external (edge) routers at the FAA facilities, connections to the backbone network, and the backbone network itself. A block diagram for the Mansfield TRACON to Marion RTR circuit is provided in Figure 5.3-1. Note that in Figure 5.3-1, the wide area network is designated as 2-hop. A hop can be defined as a connection between two network routers. In the provided example, both FAA nodes connect to the same network backbone router; therefore the wide area network consists of 2 hops. One hop is defined between the MFD external router and the network backbone router and the second between the same network backbone router and the MNN external (campus) router.

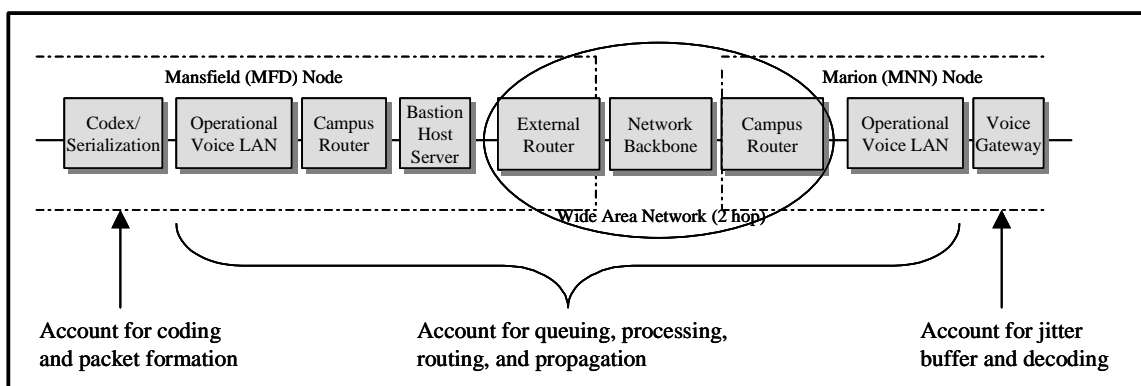


Figure 5.3-1: Latency Block Diagram - MFD TRACON to MNN RTR

Labeled in Figure 5.3-1 are the following general functions in communication processing which influence latency:

- Voice coding
- Data packetization
- Queuing
- Routing
- Propagation
- Jitter buffering
- Voice decoding

Most of these factors, as related to packet voice communication, are discussed in Section 3.2.2.2.

Using the block diagrams, latency budgets were developed for the representative latency circuits. The latency budget for the Mansfield TRACON to Marion RTR connection corresponding to Figure 5.3-1 is provided in Table 5.3-2.

The process for developing latency block diagrams and latency budgets was repeated for all of the representative circuits identified in Table 5.3-1.

Table 5.3-2: Latency Budget for MFD TRACON to MNN RTR

Source	Latency (msec)	Comment
Codex/Serialization	16.75	Assume G.729 and header compression
Operational Voice LAN (TRACON)	--	Negligible; LAN designed for contention on the order of 10's of μ sec
Campus Router	5	Assume 5 ms/Router
Bastion Host Server	--	Negligible; designed as high-end processor
Wide Area Network	16	1 msec for \approx 250 km (ITU G.141); Distance _{MFD-MNN} << 250 km Assume 5 ms/Router
<i>Propagation Delay</i>	< 1	
<i>Queuing Delay</i>	15	
Operational Voice LAN (Radio site)	--	Negligible; LAN designed for contention on the order of 10's of μ sec
Voice Gateway	107.5	Assume G.729
<i>Jitter Buffer</i>	100	
<i>Decoding Delay</i>	7.5	
Total One-Way Latency	145.25	

Appendix D includes the block diagrams and latency budget tables for these circuits. A summary of the latency analysis results is provided in Table 5.3-3.

Table 5.3-3: Latency Calculation Results Summary

Representative Scenario	Representative Circuit	Latency Budget
Terminal critical air-ground voice (TRACON to RTR)	Mansfield (MFD) TRACON to Marion (MNN) RTR	145.25 ms
En route critical air-ground voice (ARTCC to BUEC/RCAG)	ZOB ARTCC to Flint (FNT) RCAG	150.25 ms
Terminal to En Route critical A/G voice (TRACON to ARTCC)	Cleveland (CLE) TRACON to ZOB ARTCC	150.25 ms
En Route radar data (ARSR to ARTCC)	QDT ARSR to ZOB ARTCC	36 ms

In each of the voice traffic circuits analyzed, the latency attributed to communications was found to be close to the goal of 150 ms for switching and transport systems. This was true even when a small increase in latency (up to 5 ms) was added to account for architecture Scenario 1B circuits, which require an additional communications hop to access the backbone network. Keep in mind that these calculations include a conservative allocation of latency to jitter buffering. The derived values of approximately 150 ms leave a margin of approximately 100 ms to be allocated to end-system equipment and still be within the one-way end-to-end latency goal of 250 ms.

For data traffic, latency calculations do not include significant buffering and coding delays and are therefore significantly less than derived voice traffic latency values, and well below the allocation of 300 ms for critical data communication systems. The derived value, however, does not include latency

associated with the ARTCC PAMRI, which can be considered as part of the communication chain. Yet, the calculated value provides for up to 264 ms (300 ms requirement less 36 ms calculated communications latency) for PAMRI and/or other communication functions.

5.3.2 Availability Calculation

The FAA NAS availability and restoral time requirements have been presented in Sections 3.1.1 and 4.4.3. It is important to stress that the values presented in these sections are associated with end-to-end requirements rather than specific communication system allocations. The focus of this study has been on communication architectures, equipment, and interfaces with existing end-systems, but not directly on end-system performance. As such, the influence of end-system redundancy, restoral options, and end-to-end diversity on latency was not explored. To address performance of proposed communication alternatives within the scope of the study, availability was determined through a comparison of specific point-to-point circuit availability of the proposed replacement alternatives rather than on a derivation of end-to-end values and comparison to documented end-to-end availability requirements. The calculated values are only *a component* of end-to-end availability performance.

Availability can be defined as the long-term measure of the fraction of time a system meets its required performance. (A typical availability formula is provided in Section 3.2.1.1.1). This parameter is often used as a system performance indicator. Methods of achieving a high level of availability can be classified into two broad categories:

- Old World: Box Reliability
- New World: Network Availability

5.3.2.1 Box Reliability

Using box reliability, individual hardware components include redundant or standby components for each major function. Depending on exact availability requirements, different levels of fault visibility can be incorporated into a system design. These include:⁷⁷

- **Manual Masking:** Following a component fault, some manual action is required to place a redundant component into service.
- **Cold Standby:** Following a component fault, users are disconnected; and an automatic fault detection and recovery system detects the fault and brings a redundant component into service (redundant component must be initialized upon service entry).
- **Warm Standby:** Following a component fault, users of the component are disconnected; an automatic fault detection and recovery system detects the fault and notifies the redundant component to take over (redundant component has been actively running and is partially initialized).
- **Hot Standby/Active Replacement:** Active and redundant components are tightly coupled and indistinguishable to the users. Following a component fault, users are not disconnected and do not observe the fault in any way. The system continues to operate with the remaining redundant component(s) in the group providing full functionality.

With increased levels of redundancy comes less visibility of communication system faults, but significantly increased system costs.

5.3.2.2 Network Availability

The second category of availability is network availability. In this case, availability is designed into a distributed system. Some component redundancy (e.g. power supply redundancy) may be incorporated into the equipment to keep hardware failures from making a large contribution to the total failure rate, but network topology (redundant communication paths) is a significant factor in bolstering availability.

In terms of the communication architectures analyzed in this study, the baseline relies primarily on dedicated point-to-point communication paths with sufficient component-level redundancy and redundant dedicated communication paths to meet availability requirements. The proposed network architectures can use a combination of component redundancy and network redundancy to achieve availability requirements. Network redundancy is achieved by using a combination of hardware, software, and intelligent design practices to allow for automated restoral and low visibility of system faults. Sample techniques incorporated into the network to achieve desired performance include:

- Advanced Layer 3 Protocols for redirection of communication services around failures (e.g. Hot Standby Routing Protocol (HSRP) and fast converging routing protocols such as Open Shortest Path First (OSPF)).
- Advanced Layer 2 Protocols for the same purpose (e.g. tunable spanning tree parameters).

Network availability can be calculated by various means such as modeling, simulation, and measurement. Modeling was selected as the calculation method for this analysis to provide the required level of detail within the time constraints of the study.

5.3.2.2.1 Modeling Network Availability

Modeling can be performed by developing a detailed Markov analysis in which various states of a system are identified to address the working condition of key system elements. With the system states identified, the probability of transitioning from one state to another are defined. A pictorial view of a Markov state diagram (with states labeled S_{xx} and transition probabilities labels as μ_i and λ_i) is provided in Figure 5.3-2.

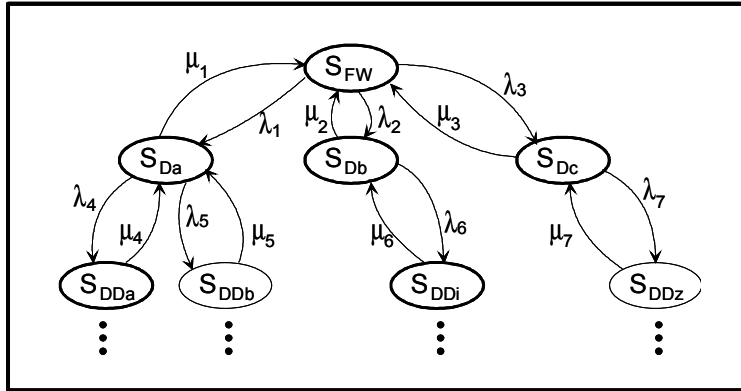


Figure 5.3-2: Example Markov State Diagram

Using Markov theory, steady state probabilities can be found. The probabilities for which the system availability goals are met are then summed to derive a system availability value. Although this approach provides a complete analysis of the different operating states of a system, detailed insight into hardware and software operation is required to create an accurate system model.

An alternate simplified modeling approach for availability is an equipment thread analysis. With this method, a series of equipment and communication links that comprise an end-to-end communication path are defined, accounting for both equipment diversity and link diversity. The availability of each component (equipment and links) in the equipment thread is defined, with all aspects of the component (e.g. hardware and software) accounted for. The joint availability of the communication string is then computed to derive system availability.

For the baseline architecture, the equipment thread approach was first used to account for the separate components of the dedicated communication paths. Then the joint (serial) availability of the entire communication path was computed.

For the proposed network architectures, a more detailed and complex model is necessary for the analysis of the backbone network performance. However, since availability is a parameter negotiated in a SLA, detailed design and analysis for the backbone is performed by the service provider(s). The remaining components of the proposed communication architectures can be identified in terms of single or redundant communication threads for interconnection of campus networks and connection of nodes to the backbone network. To avoid the complexity of a Markov analysis, the equipment thread analysis approach was also used to evaluate availability for the proposed architecture scenarios. A backbone availability value of 0.99999, corresponding to information received from several large communication service providers (see Table 3.1-3), was used in the availability analysis.

Due to the large number of circuits included in this study, a subset of communication links was selected for analysis of availability. These links are representative of communication paths with the most stringent

availability constraints. A list of representative scenarios and associated circuit examples selected for analysis is provided in Table 5.3-4.

Table 5.3-4: Availability Analysis Scenarios

Representative Scenario for Availability Analysis	Representative Architecture Circuit
Terminal critical air-ground voice (RTR to TRACON)	Marion (MNN) RTR to Mansfield (MFD) TRACON
En route critical air-ground voice (BUEC/RCAG to ARTCC)	Flint (FNT) RCAG to ZOB ARTCC
Terminal to En Route critical A/G voice (TRACON to ARTCC)	Cleveland (CLE) TRACON to ZOB ARTCC
En Route radar data (ARSR to ARTCC)	QDT ARSR to ZOB ARTCC

A set of availability block diagrams were developed for each of the circuits identified in Table 5.3-4. Each set consisted of a baseline architecture block diagram, a block diagram associated with architecture Scenarios 1A and 2, and a block diagram associated with architecture Scenario 1B. A representative set of block diagrams for the Mansfield TRACON to Marion RTR circuit is provided in Figure 5.3-3.

Using these block diagrams, a set of tables with availability calculations was developed. The availability calculations for the Marion RTR to Mansfield TRACON connections corresponding to Figure 5.3-3 are provided in Table 5.3-5, Table 5.3-6, and Table 5.3-7.

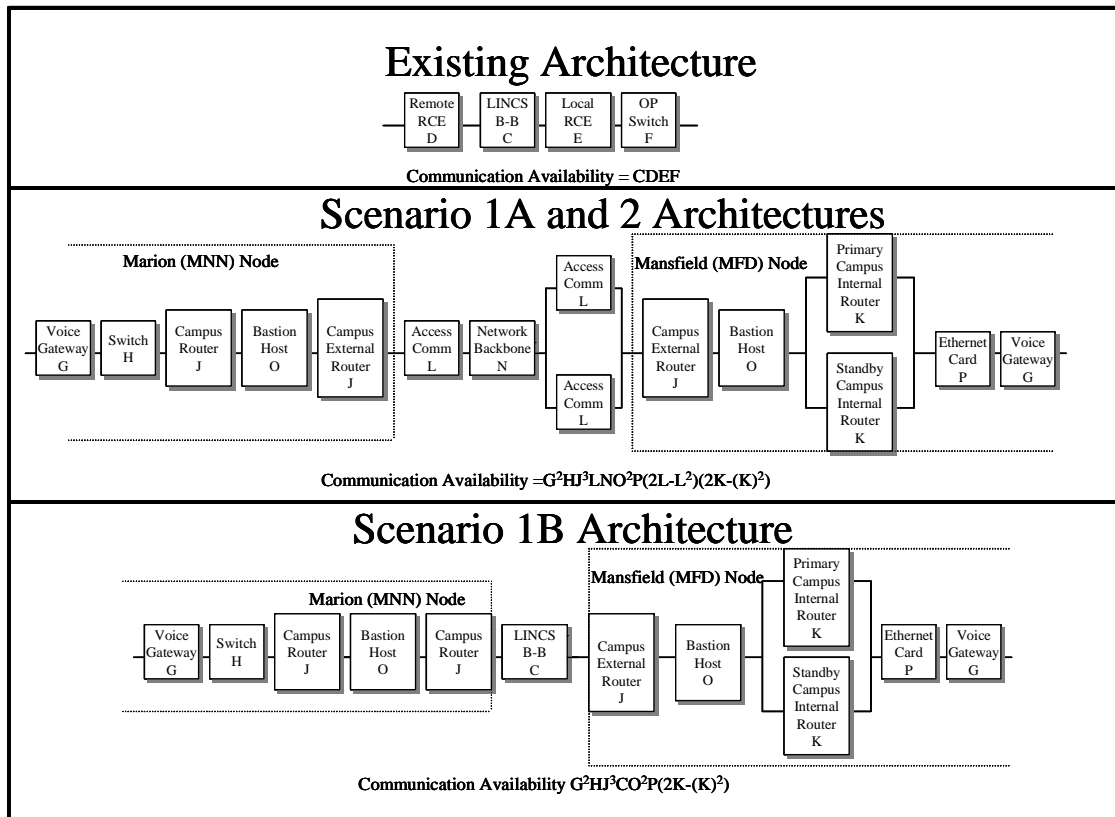


Figure 5.3-3: Availability Block Diagrams - MNN RTR to MFD TRACON

Table 5.3-5: Baseline Architecture Availability Calculation

	Item	Availability
Single Thread Comm Path		0.997859028
	Remote RCE (D)	0.99992942
	LINCS (B-B) (C)	0.998
	Local RCE (E)	0.99992942
	Op Switch (F)	0.9999999

Table 5.3-6: Architecture Scenarios 1A & 2 Availability Calculation

	Item	Availability
Total		0.997902948
<i>Campus and Access to Backbone</i>		0.997953484
	VoIP Gateway (G)	0.9999867
	Switch w/ Redundancy (H)	0.9999867
	Router w/ Redundancy (J)	0.99999333
	Bastion Host (O)	0.99999333
	Remote Access Line (L)	0.998
<i>Network Backbone</i>		0.99999
	Manged IP Network (N)	0.99999
<i>Access to Backbone and DMZ Router/Host</i>		0.99998266
	Remote Access Line (L)	0.998
	Router w/ Redundancy (J)	0.99999333
	Bastion Host (O)	0.99999333
<i>Campus Network</i>		0.9999767
	Router w/o Redundancy (K)	0.99998
	Ethernet Card (P)	0.99999
	VoIP Gateway (G)	0.9999867

Table 5.3-7: Architecture Scenario 1B Availability Calculation

	Item	Availability
Total		0.997916919
<i>Campus and Access to Backbone</i>		0.999953391
	VoIP Gateway (G)	0.9999867
	Switch w/ Redundancy (H)	0.9999867
	Router w/ Redundancy (J)	0.99999333
	Bastion Host (O)	0.99999333
<i>Leased Connection</i>		0.998
	LINCS B-B (C)	0.998
<i>DMZ Router/Host</i>		0.99998666
	Router w/ Redundancy (J)	0.99999333
	Bastion Host (O)	0.99999333
<i>Campus Network</i>		0.9999767
	Router w/o Redundancy (K)	0.99998
	Ethernet Card (P)	0.99999
	VoIP Gateway (G)	0.9999867

The process for developing availability block diagrams and associated availability calculation tables was repeated for the additional circuits identified in Table 5.3-4. Appendix D includes background information regarding specific equipment availability values as well as the block diagrams and availability calculation tables for the additional circuits. A summary of availability analysis results is provided in Table 5.3-8.

Table 5.3-8: Availability Analysis Results

Representative Scenario	Representative Circuit	Communication Link Availability		
		Baseline	Scenario 1A & 2	Scenario 1B
Terminal critical air-ground voice (RTR to TRACON)	Marion (MNN) RTR to Mansfield (MFD) TRACON	0.997859	0.997869	0.997883
En route critical air-ground voice (BUEC/RCAG to ARTCC)	Flint (FNT) RCAG to ZOB ARTCC	0.997859	0.997940	0.997940
En Route to Terminal critical A/G voice (ARTCC to TRACON)	ZOB ARTCC to Cleveland (CLE) TRACON	0.999989	0.999963	0.999963
En Route radar data (ARSR to ARTCC)	QDT ARSR to ZOB ARTCC	0.999995	0.999959	0.999939

The majority of the communications equipment implemented in the proposed network architecture are capable of automated restoral and redirection of communications around faults. The restoral time associated with the network circuit will meet or exceed the restoral performance of the baseline architecture communication circuits. In terms of availability, the proposed architecture can be designed to meet or exceed current communication performance. In some cases, CPE redundancy, as implemented in the baseline architecture, will be required.

Proposed network architectures with moderate redundancy have been developed. In a majority of the communication links, the as-proposed architecture circuits exceed availability performance of the circuits that are replaced. In some cases, as evident in the availability calculation results for CLE TRACON to ZOB and QDT to ZOB, availability performance for the as-proposed architectures is slightly less than the baseline circuits. Higher availability performance in the proposed architectures that meets or exceeds baseline performance can be achieved by adding additional redundancy in the Bastion Host Server and External Router components or by considering design alternatives with less security. This redundancy would result in marginal customer premise equipment cost increases (see Section 5.4.6.2). Due to the significant variation in availability results, analysis was repeated with added component redundancy for the CLE-ZOB and QDT-ZOB connections. The additional availability results are shown in Table 5.3-9. In these results, the CLE-ZOB connection availability value exceeds the baseline availability; for the QDT-ZOB connection, the availability value are still marginally below the baseline architecture availability. Although the availability performance itself is significantly improved with the added redundancy, the use of existing site diversity connections would need to be maintained to meet the end-to-end availability requirement for this service.

Table 5.3-9: Availability Calculations - Added Component Redundancy

Representative Connection	Baseline Architecture	Scenario 1A and 2 Architecture	Scenario 2 Architecture
CLE TRACON to ZOB ARTCC	0.999989	0.9999899	0.9999899
QDT ARSR to ZOB ARTCC	0.999995	0.9999859*	0.9999859*

*These values are lower than the baseline connection value, however, with the site diversity, the end-to-end service availability requirement would still be met.

5.4 COST ANALYSIS AND COMPARISON

The following subsections describe the focus of the cost analysis; describe a methodology for performing cost calculations for the candidate network communication architectures; and document cost analysis results.

5.4.1 Focus of the Cost Analysis

The focus of the cost analysis was the comparison of circuit monthly recurring charges (MRCs) among the candidate communication architectures and the communication baseline. The MRC provides a metric of the long-term cost effects of the different communication implementations.

In addition to circuit costs, key network customer premise equipment (CPE) used to form campus area networks at the FAA nodes and to provide the interface between the FAA nodes and the backbone network was also identified and priced. This study did not include FAA site surveys to determine the specific state of existing communication equipment, replacement schedules, equipment operation and maintenance costs, and replacement system costs. Therefore, the derived CPE costs for implementing campus area networks and providing connection to the backbone network cannot be compared to a baseline CPE scenario.

5.4.2 Circuit Cost Calculations

Circuit MRCs were calculated for baseline architecture scenarios as well as for each of the proposed architecture scenarios (Scenario 1A, Scenario 1B, and Scenario 2). A description of the methodology used to develop a circuit cost model and the results of the exercise of the model are presented as follows:

- Section 5.4.2.1: Baseline Communication Architecture Circuit MRC.
- Section 5.4.2.2: Network Architecture Scenario 1A Circuit MRC.
- Section 5.4.2.3: Network Architecture Scenario 1B Circuit MRC.
- Section 5.4.2.4: Network Architecture Scenario 2 Circuit MRC.

5.4.2.1 Baseline Communication Architecture Circuit MRC

The baseline architecture costs were found using information obtained in a download from the FAA TIMS database dated June 9, 2000. The TIMS database is a record of FAA leased circuits ordered through and contracted by DITCO. FAA-owned resources (e.g. RCL, LDRCL) and circuits leased without DITCO involvement (e.g. some regional circuits and some FTS2000 circuits) were not included.

For each FAA facility included for analysis, database queries were developed to identify communication circuits. Circuits were catalogued and given a unique circuit identifier, i.e. E.1, E.2 for existing circuit number 1 and existing circuit number 2, respectively. MRCs for each unique circuit were extracted from the TIMS database download. An excerpt of the list of baseline architecture circuits associated with the FAA facilities selected for study and corresponding MRCs is provided in Table 5.4-1. The list is shown in its entirety in Appendix C.

The baseline communication architecture for the region under study includes 874 unique circuits. The total MRC associated with these circuits is \$231,474.

Table 5.4-1: Excerpt from Baseline Communication Architecture Circuit List with MRC

Circuit Number	Termination Node 1	Termination Node 2	External I/F?	Service	Comment	Cost
E.20	ADG	AG8	N	ASOS	Voice Grade Circuit	\$644.51
E.21	MBS TRACON	AMN RTR	N	TCOM		\$163.82
E.22	DTW TRACON	ARB RTR	N	TCOM		\$115.38
E.23	DTW TRACON	ARB ATCT	N	DMN	Voice Grade Circuit; DMN carrying FDIO, DBRITE, ASOS, & DCX	\$107.97
E.24	ZOB	MTC BASOP	N	SVFB		\$255.35
E.25	DTW TRACON	ARB ATCT	N	SVFC	MISC - Assumed SVFC	\$107.97
E.26	ARB ATCT	AH8	N	ATIS	ATIS recorder connection at ARB	\$143.63
E.27	DTW TRACON	ARB ATCT	N	METI	AWIS connection at ARB	\$107.97
E.28	DTW TRACON	ARB ATCT	N	SVFC	Operational Switch connection at ARB	\$115.38
E.29	LAN AFSS	BAX RCO	N	FCOM		\$237.38
E.30	CAK TRACON	BJJ RTR	Y	TCOM		\$460.71
E.31	ZOB	BJJ ASOS	N	ASOS	Voice Grade Circuit	\$335.72
E.32	ZID	CLE ARSR	Y	DMN		\$419.67
E.33	ZOB	CLE ARSR	N	DMN		\$115.66
E.34	CLE TRACON	CLE WSFO	N	DMN		\$55.94
E.35	CLE AFSS	MFD VOR	N	FCOM		\$269.66
E.36	CLE AFSS	CXR VOR	Y	FCOM		\$126.63
E.37	CLE AFSS	AGC RCO	Y	EFAS		\$242.16
E.38	CLE AFSS	AGC RCO	Y	EFAS		\$242.16
E.39	CLE AFSS	FDY VOR	N	FCOM		\$279.12
E.40	CLE AFSS	AIR VOR	Y	FCOM		\$374.45

To gain insight into the distribution of circuit costs among general functional categories of FAA services as well as specific FAA services documented in the *Current FAA Telecommunication System and Facility Description Manual, Currant Book*, the baseline circuits were analyzed in terms of number of circuits and circuit cost. The distribution of baseline circuits analyzed in terms of number of operational voice circuits, administrative voice circuits, operational data circuits, and administrative data circuits is shown in Figure 5.4-1.

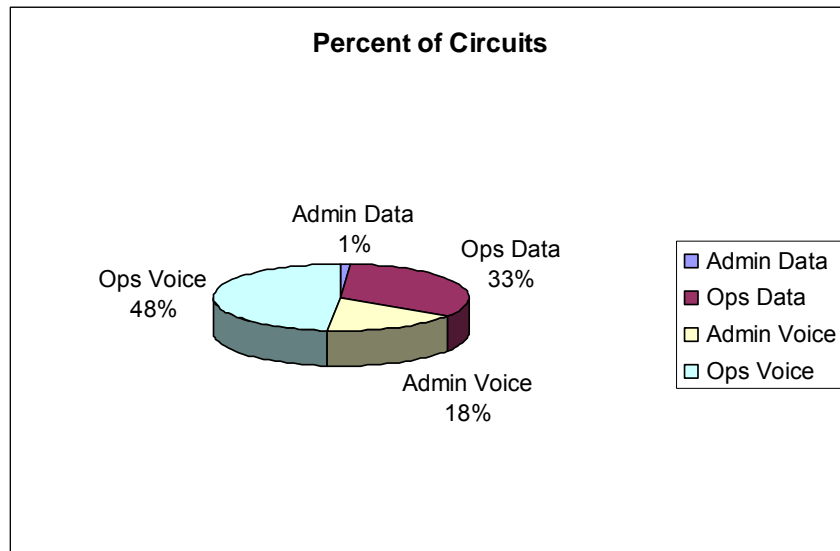


Figure 5.4-1: Allocation of Baseline Circuits (Number of Circuits)

The cost associated with each of these general categories of baseline circuits was also computed. The distribution of costs between data and voice circuits is similar to the distribution of number of circuits, however the allocation of cost between operation and administrative functions is significantly shifted. The distribution of circuit costs among operational voice, administrative voice, operational data, and administrative data for the baseline circuits analyzed is shown in Figure 5.4-2.

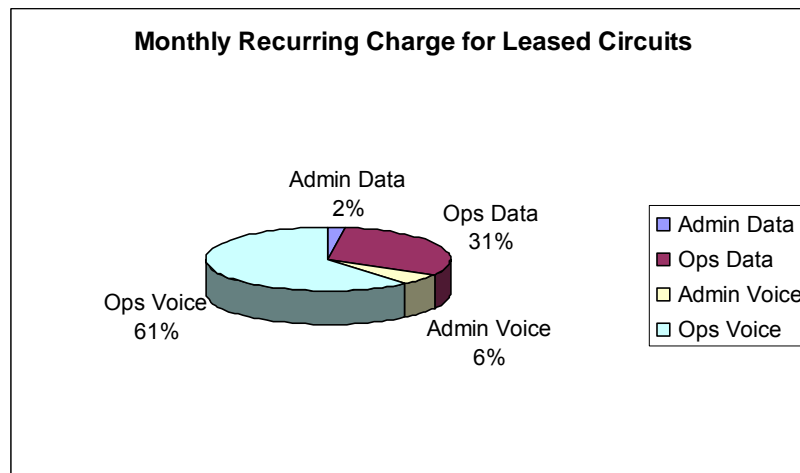


Figure 5.4-2: Allocation of Baseline Circuit Costs

The specific distribution of operational voice and operational data circuits in terms of circuit costs by FAA service category were also identified. These distributions are provided in Figure 5.4-3.

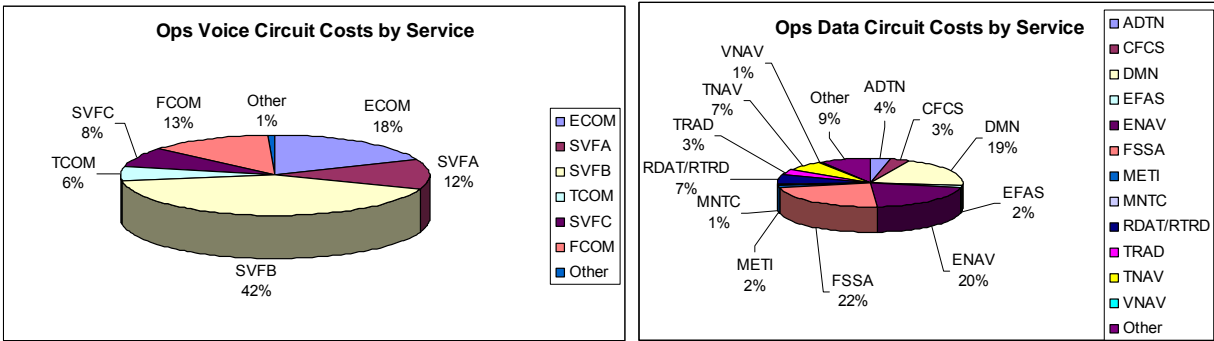


Figure 5.4-3: Distribution of Operational Circuit Costs

5.4.2.2 Network Architecture Scenario 1A Circuit MRC

Using the node diagrams created as part of the network architecture description, a unique set of circuits for Scenario 1A were identified and documented. These circuits provided the same logical connectivity to the FAA facilities analyzed as the circuits included in the baseline architecture and include a mixture of on-campus circuits for the FAA nodes as well as connections between the node and the nearest backbone POP.

For each Scenario 1A circuit, the end-point telecommunication location identifier information (i.e. area code/exchange, NPA/NXX) parameters were found. These parameters were also identified for the backbone POP locations. Additionally, the bandwidth requirement for each circuit was derived based on the FAA services carried on the circuit. As noted in Section 4.4.3, references used to derive bandwidth requirements included:

- *Current FAA Telecommunication Systems and Facility Description Manual, Currant Book*, Fiscal Year 1999 Edition, NAS Operations (AOP) Telecommunications Support and International Communications Division.
- *Future FAA Telecommunications Plan, Fuschia Book*, NAS Operations (AOP) Telecommunications Network Planning and Engineering Division, April 2000.
- NAS-SS-1000.
- NAS-SR-1000.

With the circuits and associated data compiled, circuits were priced by one of three methods depending on the applicable case, as summarized in Table 5.4-2.

Using the methodology and tools identified in Table 5.4-2, circuit MRCs were computed for the 175 circuits that comprise architecture Scenario 1A. An excerpt of the list of circuits and associated prices is shown in Table 5.4-3.

Table 5.4-2: Scenario 1A Pricing Methods and Tools

Pricing Case	Pricing Method and Tool
1) Circuits Identical to Backbone Architecture	Using existing circuit MRC based on TIMS download data
2) Campus Circuits (initiating and terminating at FAA facilities)	The FAA LINC'S pricing tool, FLAPS, was used to calculated circuit MRCs
3) Node Connections to the Backbone POP	To estimated commercial network access costs, the FTS-2001 Pricing Tool (SDP Pricer) was used with Year 3 prices.

A complete list of the Scenario 1A circuits is provided in Appendix C. The total MRC for campus connections and network access for the Scenario 1A circuits is \$125,138.

Table 5.4-3: Scenario 1A Circuits and Prices

Circuit Number	End Point 1	End Point 2	External Connection?	Service	Access Line/ Campus Line	Access Line NRC	Access Line MRC	Cost Tool
S1A.1	AA8	PSTN	Y	ADVO	Original	--	\$43.08	TIMS
S1A.2	AB8	PSTN	Y	ADVO	Original	--	\$39.49	TIMS
S1A.3	AC8	PSTN	Y	ADVO	Original	--	\$56.06	TIMS
S1A.4	ADG	TOL POP	Y	ASOS	DS0	\$1,462.64	\$265.06	SDP Pricer
S1A.5	AE8	PSTN	Y	ADVO	Original	--	\$70.38	TIMS
S1A.6	AMN	Battle Creek POP	Y	TCOM	DS0	\$1,462.64	\$327.18	SDP Pricer
S1A.7	ARB RTR	ARB ATCT	N	TCOM	DDS-56/64	\$1,503.93	\$191.66	FLAPS
S1A.8A	ARB ATCT	Plymouth POP	Y	TCOM, DMN, SVFC, ATIS, METI, ADVO, ASOS, SVFB	256 kbps (DS0x4)	\$2,885.63	\$1,060.73	SDP Pricer
S1A.8B	ARB ATCT	Plymouth POP	Y	TCOM, DMN, SVFC, ATIS, METI, ADVO, ASOS, SVFB	256 kbps (DS0x4)	\$2,885.63	\$1,060.73	SDP Pricer
S1A.9	BAX	Detroit POP	Y	FCOM	DS0	\$1,462.64	\$268.38	SDP Pricer
S1A.10	BJJ	Cleveland POP	Y	TCOM, ASOS	DS0	\$1,462.64	\$313.30	SDP Pricer
S1A.11	CLE ARSR	CLE TRACON	N	DMN (RDAT)	DDS-56/64	\$2,050.72	\$302.05	FLAPS
S1A.12	CLE ARSR	CLE TRACON	N	DMN (RDAT)	DDS-56/64	\$2,050.72	\$302.05	FLAPS
S1A.13	CLE WSFO	CLE TRACON	N	ASOS, METI, ADVO	DDS-56/64	\$2,050.72	\$309.03	FLAPS
S1A.14A	CLE OM	CLE TRACON	N	TNAV	Original	--	\$101.25	TIMS
S1A.14B	CLE OM	CLE TRACON	N	TNAV	Original	--	\$101.25	TIMS
S1A.15A	CLE TDWR	CLE TRACON	N	TDWR	Original	--	\$148.50	TIMS
S1A.15B	CLE TDWR	PSTN	N	ADVO	Original	--	\$138.17	TIMS
S1A.16	CLE RCO	CLE TRACON	N	FCOM	DDS-56/64	\$2,050.72	\$308.15	FLAPS
S1A.17	CLE CASFU	CLE TRACON	N	ADVO	FB-256	\$2,498.59	\$1,104.96	FLAPS
S1A.18	CLE MIDO	RGC HDQ	Y	ADTN	Original	--	\$690.24	TIMS
S1A.19	CLE FSDO	RGC HDQ	Y	ADTN	Original	--	\$339.24	TIMS
S1A.20	CLE SSU	PSTN	Y	ADVO	Original	--	\$33.70	TIMS
S1A.21	CLE AFSS	CLE TRACON	N	multiple	DS1	\$3,213.60	\$1,189.55	FLAPS
S1A.22	CLE TRACON	Cleveland POP	Y	multiple	DS1x3	\$9,216.59	\$4,285.92	SDP Pricer
S1A.23	CLE TRACON	Cleveland POP	Y	multiple	DS1x3	\$9,216.59	\$4,285.92	SDP Pricer
S1A.24	CRL RCO	CRL RCAG	N	FCOM, ADVO	DDS-56/64	\$1,503.93	\$191.66	FLAPS
S1A.25A	CRL	Detroit POP	Y	ECOM, ADVO, FCOM	128 kbps (DS0x2)	\$2,885.63	\$454.97	SDP Pricer
S1A.25B	CRL	Detroit POP	Y	ECOM, ADVO, FCOM	128 kbps (DS0x2)	\$2,885.63	\$454.97	SDP Pricer
S1A.26	DET-1 IBP	ZMP TRACON	Y	FDAT	Original	--	\$114.00	TIMS
S1A.27	DET-1 IBP	DTW TRACON	Y	FDAT	Original	--	\$69.98	TIMS
S1A.28	DET-1 IBP	Plymouth POP	Y	SVFB, SVFC	DS0	\$1,462.64	\$271.41	SDP Pricer
S1A.29	DET-1 IBP	Plymouth POP	Y	SVFB, SVFC	DS0	\$1,462.64	\$271.41	SDP Pricer
S1A.30	DET-2 RCO	DET-2 ATCT	N	FCOM	DDS-56/64	\$1,503.93	\$191.66	FLAPS
S1A.31	DET-2	Detroit POP	Y	DBRITE, NRCS, METI, SVFC, ASOS, ADVO, FCOM, EFAS	DS1x3	\$9,216.59	\$7,387.44	SDP Pricer
S1A.32	DET-2	Detroit POP	Y	DBRITE, NRCS, METI, SVFC, ASOS, ADVO, FCOM, EFAS	DS1x3	\$9,216.59	\$7,387.44	SDP Pricer
S1A.33	DFI	Toledo POP	Y	ASOS	DS0	\$1,464.64	\$600.31	SDP Pricer
S1A.34	DJB RTR	22G ARPT	N	TCOM, FCOM	DDS-56/64	\$1,503.93	\$218.95	FLAPS
S1A.35	DJB	Cleveland POP	Y	TCOM, FCOM, ASOS	DS0	\$1,464.64	\$217.44	SDP Pricer
S1A.36	ECK	Detroit POP	Y	FCOM, ADVO	DS0	\$1,464.64	\$254.32	SDP Pricer
S1A.37	FDY RCAG	FDY FSS	N	ECOM	FB-128	\$1,371.07	\$537.91	FLAPS
S1A.38	FDY RCAG	FDY FSS	N	ECOM	FB-128	\$1,371.07	\$537.91	FLAPS
S1A.39	FDY RCO/VTAC	FDY FSS	N	FCOM, EFAS, ADVO	DDS-56/64	\$1,503.93	\$221.16	FLAPS
S1A.40	FDY RTR/ASOS	FDY FSS	N	TCOM, ASOS, AWOS	DDS-56/64	\$1,503.93	\$191.66	FLAPS

5.4.2.3 Network Architecture Scenario 1B Circuit MRC

Recall the significant difference between architecture Scenarios 1A and 1B is that for 1B, only larger FAA facilities (ARTCCs, Level 4/5 TRACONs, and additional TRACONs central to many smaller FAA facilities) connect to the commercial backbone network. These large facilities are considered regional hub sites, while the smaller FAA facilities in the vicinity connect to the backbone network via the hub nodes. The connections between the smaller FAA facilities and FAA hub nodes is via dedicated leased communications.

Similar to the procedure used for pricing Scenario 1A circuits, a unique set of connections were identified based on the node diagrams for Scenario 1B. Next, circuit end-point telecommunication identifier information (NPA/NXX) and bandwidth requirements for the circuits were obtained in a manner similar to the procedure described for Scenario 1A (See section 5.4.2.2). The different cases and associated cost analysis methodology and tools for Scenario 1B circuits are summarized in Table 5.4-4.

Table 5.4-4: Scenario 1B Pricing Methods and Tools

Pricing Case	Pricing Method and Tool
1) Circuits Identical to Backbone Architecture	Using existing circuit MRC based on TIMS download data
2) Campus Circuits (initiating and terminating at FAA facilities) and Connection of Small FAA Nodes to FAA Hub Nodes	The FAA LINCS pricing tool, FLAPS, was used to calculate circuit MRCs
3) Hub Node Connections to the Backbone POP	To estimate commercial network access costs, the FTS-2001 Pricing Tool (SDP Pricer) was used with Year 3 prices.

The resulting MRC for campus network connections, interconnection of FAA nodes, and connection of hub nodes to the backbone network for the 175 circuits that comprise Scenario 1B is \$104,086. An excerpt from the Scenario 1B circuit list is provided in Table 5.4-5. The complete list of circuits is provided in Appendix C.

5.4.2.4 Network Architecture Scenario 2 Circuit MRC

The costing methodology for architecture Scenario 2 is similar to the procedure developed for architecture Scenario 1A (see Section 5.4.2.2). The significant difference between the two architectures is the location of the backbone network access locations. For Scenario 1A, a low-density POP backbone network is used. In Scenario 2, the forecasted expansion of commercial network services is accounted for, and a high-density POP backbone network is used. For this case, it is assumed that the connection to the nearest network POP is local.

In Scenario 1A, the FTS-2001 pricing tool (SDP Pricer) was used for determining both circuit set-up charges and MRCs for connection of nodes to the backbone network. However, when the tool is used to cost connections within a designated NPX/NXX region (i.e. backbone POP is in same calling area as FAA node), costs are inflated without explanation. Therefore, to determine the MRC for connecting nodes to the backbone for Scenario 2, the FLAPS pricing tool was utilized.

Table 5.4-5: Scenario 1B Circuits and Prices

Circuit Number	End Point 1	End Point 2	External Connection?	Service	Access Line/ Campus Line	Access Line NRC	Access Line MRC	Cost Tool
S1B.1	AA8	PSTN	Y	ADVO	Original	--	\$43.08	TIMS
S1B.2	AB8	PSTN	Y	ADVO	Original	--	\$39.49	TIMS
S1B.3	AC8	PSTN	Y	ADVO	Original	--	\$56.06	TIMS
S1B.4	ADG	Toledo TRACON	Y	ASOS	DS0	\$2,050.72	\$654.30	FLAPS
S1B.5	AE8	PSTN	Y	ADVO	Original	--	\$70.38	TIMS
S1B.6	AMN	MBS TRACON	Y	TCOM	DS0	\$1,503.93	\$248.23	FLAPS
S1B.7	ARB RTR	ARB ATCT	N	TCOM	DDS-56/64	\$1,503.93	\$191.66	FLAPS
S1B.8A	ARB ATCT	DTW TRACON	Y	TCOM, DMN, SVFC, ATIS, METI, ADVO, ASOS, SVFB	DS0x4 or DS1	\$2,292.34	\$445.24	FLAPS
S1B.8B	ARB ATCT	DTW TRACON	Y	TCOM, DMN, SVFC, ATIS, METI, ADVO, ASOS, SVFB	DS0x4 or DS1	\$2,292.34	\$445.24	FLAPS
S1B.9	BAX	MBS TRACON	Y	FCOM	DS0	\$1,503.93	\$271.35	FLAPS
S1B.10	BJJ	MFD TRACON	Y	TCOM, ASOS	DS0	\$1,378.56	\$404.25	FLAPS
S1B.11	CLE ARSR	CLE TRACON	N	DMN (RDAT)	DDS-56/64	\$2,050.72	\$302.05	FLAPS
S1B.12	CLE ARSR	CLE TRACON	N	DMN (RDAT)	DDS-56/64	\$2,050.72	\$302.05	FLAPS
S1B.13	CLE WSFO	CLE TRACON	N	ASOS, METI, ADVO	DDS-56/64	\$2,050.72	\$309.03	FLAPS
S1B.14A	CLE OM	CLE TRACON	N	TNAV	Original	--	\$101.25	TIMS
S1B.14B	CLE OM	CLE TRACON	N	TNAV	Original	--	\$101.25	TIMS
S1B.15A	CLE TDWR	CLE TRACON	N	TDWR	Original	--	\$148.50	TIMS
S1B.15A	CLE TDWR	CLE TRACON	N	ADVO	Original	--	\$138.17	TIMS
S1B.16	CLE RCO	CLE TRACON	N	FCOM	DDS-56/64	\$2,050.72	\$308.15	FLAPS
S1B.17	CLE CASFU	CLE TRACON	N	ADVO	FB-256	\$2,498.59	\$1,104.96	FLAPS
S1B.18	CLE MIDO	RGC HDQ	Y	ADTN	Original	--	\$690.24	TIMS
S1B.19	CLE FSDO	RGC HDQ	Y	ADTN	Original	--	\$339.24	TIMS
S1B.20	CLE SSU	PSTN	Y	ADVO	Original	--	\$33.70	TIMS
S1B.21	CLE AFSS	CLE TRACON	N	multiple	DS1	\$3,213.60	\$15.00	FLAPS
S1B.22	CLE TRACON	ZOB ARTCC	Y	multiple	DS1x3 or DS3	\$9,640.80	\$1,173.84	FLAPS
S1B.23	CLE TRACON	ZOB ARTCC	Y	multiple	DS1x3 or DS3	\$9,640.80	\$1,173.84	FLAPS
S1B.24	CRL RCO	CRL RCAG	N	FCOM, ADVO	DDS-56/64	\$1,503.93	\$191.66	FLAPS
S1B.25A	CRL	DTW TRACON	N	ECOM, ADVO, FCOM	FB-128	\$2,292.34	\$326.60	FLAPS
S1B.25B	CRL	DTW TRACON	N	ECOM, ADVO, FCOM	FB-128	\$2,292.34	\$326.60	FLAPS
S1B.26	DET-1 IBP	ZMP TRACON	Y	FDAT	Original	--	\$114.00	TIMS
S1B.27	DET-1 IBP	DTW TRACON	Y	FDAT	Original	--	\$69.98	TIMS
S1B.28	DET-1 IBP	LAN TRACON	Y	SVFB, SVFC	DS0	\$2,050.72	\$260.42	FLAPS
S1B.29	DET-1 IBP	LAN TRACON	Y	SVFB, SVFC	DS0	\$2,050.72	\$260.42	FLAPS
S1B.30	DET-2 RCO	DET-2 ATCT	N	FCOM	DDS-56/64	\$1,503.93	\$191.66	FLAPS
S1B.31	DET-2	DTW TRACON	Y	DBRITE, NRCS, METI, SVFC, ASOS, ADVO, FCOM, EFAS	DS1x3 or DS3	\$6,877.01	\$1,925.88	FLAPS
S1B.32	DET-2	DTW TRACON	Y	DBRITE, NRCS, METI, SVFC, ASOS, ADVO, FCOM, EFAS	DS1x3 or DS3	\$6,877.01	\$1,925.88	FLAPS
S1B.33	DFI	Toledo TRACON	Y	ASOS	DS0	\$1,856.97	\$162.57	FLAPS
S1B.34	DJB RTR	22G ARPT	N	TCOM, FCOM	DDS-56/64	\$1,503.93	\$218.95	FLAPS
S1B.35	DJB	ZOB ARTCC	Y	TCOM, FCOM, ASOS	DS0	\$1,856.97	\$132.72	FLAPS

After running a representative set of cost scenarios, it was determined that the cost of a local connection within a NPX/NXX region was generally based on type (size) of circuit, regardless of location. Based on the FLAPS cost output for the representative circuit set, MRC values based on connection types were assigned. These MRCs were used in the Architecture Scenario 2 analysis and are documented in Table 5.4-6.

Table 5.4-6: MRC for Node Connection to Backbone POPs (Scenario 2)

Local Connection to Backbone POP within a NPX/NXX region	
Connection Type	Monthly Recurring Charge
DS-0	\$200.00
F-T1, T1	\$470.00
Multiple T1	\$3000.00

A summary of the pricing methods used for the Scenario 2 cost analysis is provided in Table 5.4-7.

Table 5.4-7: Scenario 2 Pricing Methods and Tools

Pricing Case	Pricing Method and Tool
1) Circuits Identical to Backbone Architecture	Using existing circuit MRC based on TIMS download data
2) Campus Circuits (initiating and terminating at FAA facilities)	The FAA LINCS pricing tool, FLAPS, was used to calculate circuit MRCs
3) Node Connections to the Backbone POP	Values derived from the FAA LINCS pricing tool, FLAPS (See Table 5.4-6)

An excerpt from the Scenario 2 circuit list is provided in Table 5.4-8. The list is shown in its entirety in Appendix C. The MRC for the campus circuits and network access circuits for the 175 circuits comprising the Scenario 2 connections is \$72,417.

5.4.3 Backbone Usage Costs and Other Cost Considerations

Before the costs identified in Sections 5.4.2.2, 5.4.2.3, and 5.4.2.4 above can be compared to the baseline architecture, several factors need to be accounted for:

- **Backbone network usage charges:** account for service provider charges for actual backbone traffic.
- **Network access charges for circuit end-point not in the representative architecture:** For circuits that have one termination location not within the representative architecture, account for connections from the remote end-point to the backbone network.

These factors are addressed in the following subsections.

5.4.3.1 Backbone Network Usage Charges

In order to provide a comparison of circuit MRCs between the proposed architecture scenarios and the baseline architecture MRC, the costs associated with traffic on the backbone network need to be accounted for and added to the campus circuit and node access circuit costs derived in Section 5.4.2 for each proposed network architecture.

Backbone usage MRC values were derived based on cost data associated with four large telecommunication service providers, namely GTE, Uunet, Qwest, & Infonet.⁷⁸ In the cost reference, total telecommunication costs for private IP services were identified for several national and international cities. Only costs associated with the two cities located within the U.S. were used for analysis.

Table 5.4-8: Scenario 2 Circuits and Prices

Circuit Number	End Point 1	End Point 2	External Connection?	Service	Access Line/Campus Line	Access Line NRC	Access Line MRC	Cost Tool
S2.1	AA8	PSTN	Y	ADVO	Original	--	\$43.08	TIMS
S2.2	AB8	PSTN	Y	ADVO	Original	--	\$39.49	TIMS
S2.3	AC8	PSTN	Y	ADVO	Original	--	\$56.06	TIMS
S2.4	ADG	Adrian POP	Y	ASOS	DS0	\$1,462.64	\$200.00	SDP Pricer
S2.5	AE8	PSTN	Y	ADVO	Original	--	\$70.38	TIMS
S2.6	AMN	Alma POP	Y	TCOM	DS0	\$1,462.64	\$200.00	SDP Pricer
S2.7	ARB RTR	ARB ATCT	N	TCOM	DDS-56/64	\$1,503.93	\$191.66	FLAPS
S2.8A	ARB ATCT	Ann Arbor POP	Y	TCOM, DMN, SVFC, ATIS, METI, ADVO, ASOS, SVFB	256 kbps (DS0x4)	\$2,885.63	\$470.00	SDP Pricer
S2.8B	ARB ATCT	Ann Arbor POP	Y	TCOM, DMN, SVFC, ATIS, METI, ADVO, ASOS, SVFB	256 kbps (DS0x4)	\$2,885.63	\$470.00	SDP Pricer
S2.9	BAX	Bad Axe POP	Y	FCOM	DS0	\$1,462.64	\$200.00	SDP Pricer
S2.10	BJJ	Smithville POP	Y	TCOM, ASOS	DS0	\$1,462.64	\$200.00	SDP Pricer
S2.11	CLE ARSR	CLE TRACON	N	DMN (RDAT)	DDS-56/64	\$2,050.72	\$302.05	FLAPS
S2.12	CLE ARSR	CLE TRACON	N	DMN (RDAT)	DDS-56/64	\$2,050.72	\$302.05	FLAPS
S2.13	CLE WSFO	CLE TRACON	N	ASOS, METI, ADVO	DDS-56/64	\$2,050.72	\$309.03	FLAPS
S2.14A	CLE OM	CLE TRACON	N	TNAV	Original	--	\$101.25	TIMS
S2.14B	CLE OM	CLE TRACON	N	TNAV	Original	--	\$101.25	TIMS
S2.15A	CLE TDWR	CLE TRACON	N	TDWR	Original	--	\$148.50	TIMS
S2.15B	CLE TDWR	PSTN	N	ADVO	Original	--	\$138.17	TIMS
S2.16	CLE RCO	CLE TRACON	N	FCOM	DDS-56/64	\$2,050.72	\$308.15	FLAPS
S2.17	CLE CASFU	CLE TRACON	N	ADVO	FB-256	\$2,498.59	\$1,104.96	FLAPS
S2.18	CLE MIDO	RGC HDQ	Y	ADTN	Original	--	\$690.24	TIMS
S2.19	CLE FSDO	RGC HDQ	Y	ADTN	Original	--	\$339.24	TIMS
S2.20	CLE SSU	PSTN	Y	ADVO	Original	--	\$33.70	TIMS
S2.21	CLE AFSS	CLE TRACON	N	multiple	DS1	\$3,213.60	\$1,189.55	FLAPS
S2.22	CLE TRACON	Cleveland POP	Y	multiple	DS1x3	\$9,216.59	\$3,000.00	SDP Pricer
S2.23	CLE TRACON	Cleveland POP	Y	multiple	DS1x3	\$9,216.59	\$3,000.00	SDP Pricer
S2.24	CRL RCO	CRL RCAG	N	FCOM, ADVO	DDS-56/64	\$1,503.93	\$191.66	FLAPS
S2.25A	CRL	Carlton POP	Y	ECOM, ADVO, FCOM	128 kbps (DS0x2)	\$2,885.63	\$470.00	SDP Pricer
S2.25B	CRL	Carlton POP	Y	ECOM, ADVO, FCOM	128 kbps (DS0x2)	\$2,885.63	\$470.00	SDP Pricer
S2.26	DET-1 IBP	ZMP TRACON	Y	FDAT	Original	--	\$114.00	TIMS
S2.27	DET-1 IBP	DTW TRACON	Y	FDAT	Original	--	\$69.98	TIMS
S2.28	DET-1 IBP	Manchester POP	Y	SVFB, SVFC	DS0	\$1,462.64	\$200.00	SDP Pricer
S2.29	DET-1 IBP	Manchester POP	Y	SVFB, SVFC	DS0	\$1,462.64	\$200.00	SDP Pricer
S2.30	DET-2 RCO	DET-2 ATCT	N	FCOM	DDS-56/64	\$1,503.93	\$200.00	FLAPS

The total telecommunication costs identified by the service providers were allocated to cost functions based on an actual allocation of costs incurred during the recent implementation of a state government IP WAN and establishment of connections to the network.⁷⁹ This allocation of costs is provided in Figure 5.4-4.

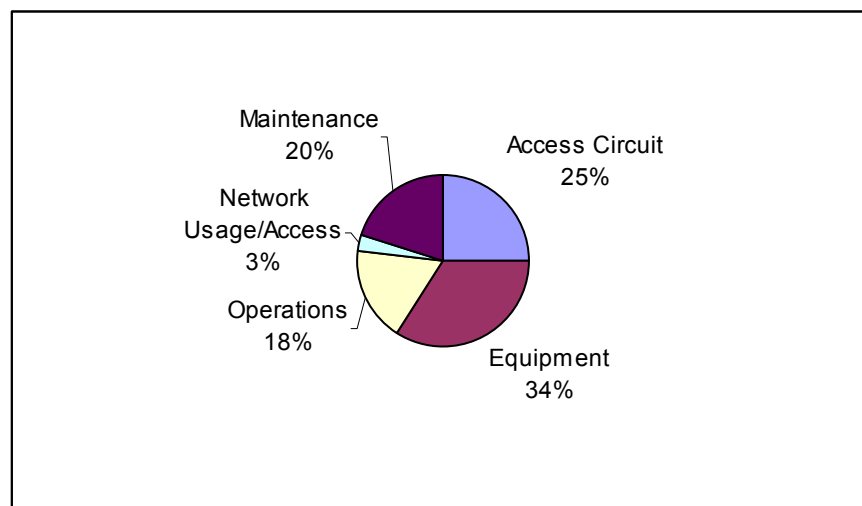


Figure 5.4-4: Allocation of Network Access Communication Costs

Given this allocation, network usage costs account for approximate 3% of the communication costs. To provide a margin of error, a value of 5% of total service costs were assumed to represent backbone usage costs.

This percentage was applied to the costs identified for the four network service providers noted above for both a T-1 connection and a 56-kbps connection (as indicated in the referenced article). The costs for the different service providers were then averaged to derive a backbone usage costs. This procedure is summarized in Table 5.4-9.

Table 5.4-9: Backbone Usage Charge Calculation

Backbone Usage Charge: T1 and 56 kbps			
T1	Approximated Total Cost (T1 connection at NY)	5% Allocation For Network Usage	Average T1 Usage Cost
Qwest	\$1700	\$75	\$128
Uunet	\$2600	\$130	
PSInet	\$3800	\$190	
GTE	\$2300	\$115	
	Approximated Total Cost (56 kbps connection at NY)	5% Allocation For Network Usage	Average 56kbps Usage Cost
Qwest	\$300	\$15	\$40
Uunet	\$1100	\$55	
PSInet	\$700	\$35	
GTE	\$1100	\$55	

To define backbone usage charges associated with other connection data rates, charges were scaled uniformly. The resulting set of network backbone charges for the three architecture scenarios are provided in Table 5.4-10.

Table 5.4-10: Backbone Usage Cost Development

Backbone Connection	Associated Backbone Usage Charge	Scenarios 1A and 2		Scenario 1B	
		Number of Connections	Total Cost/Connection	Number of Connections	Total Cost/Connection
56 kbps	\$40/month	20	\$800.00	0	\$0.00
128 kbps	\$45/month	7	\$315.00	0	\$0.00
256 kbps	\$52/month	2	\$104.00	0	\$0.00
512 kbps	\$70/month	3	\$210.00	2	\$140.00
768 kbps	\$83/month	1	\$83.00	1	\$83.00
T1	\$128/month	1	\$128.00	0	\$0.00
2xT1	\$256/month	2	\$512.00	2	\$512.00
3xT1	\$384/month	2	\$768.00	0	\$0.00
3xT1	\$512/month	1	\$512.00	0	\$0.00
6xT1	\$768/month	1	\$768.00	1	\$768.00
7xT1	\$896/month	0	\$0.00	1	\$896.00
		Total:	\$4,200.00	Total:	\$2,399.00

The low total cost associated with backbone usage is consistent with decreased commercial bandwidth charges attributed to the bandwidth efficiencies gained with new and emerging data transport technologies such as dense wave-division multiplexing. Based on the backbone usage charges computed in Table 5.4-10 and rounding up to the nearest thousand to provide a small margin for error, a MRC for

backbone usage of \$5,000 was used for architecture scenarios 1A and 2, and a MRC of \$3,000 was used for architecture scenario 2.

5.4.3.2 Network Access Charges for Distance Circuit End-Points

The baseline circuits included in the cost analysis include the price of the complete communication connection between two FAA circuit end-points. Of these circuits, 67% have both circuit end-points within FAA sites selected for analysis. The remaining 33% connect to approximately 80 different FAA facilities located outside the area of study.

The circuit MRC identified in Sections 5.4.2.2, 5.4.2.3, and 5.4.2.4 for the proposed network architecture scenarios include connections of FAA nodes (comprised of sites selected for analysis) to the backbone network. To be able to compare these circuit costs with those for the baseline architecture, facility-to-facility connection costs need to be considered. This includes the cost for sites not selected for analysis to connect to the backbone network to complete their connection with nodes within the representative architecture. Without detailed analysis of the additional 80 FAA facilities, assigning a specific cost to network access for those sites presents a difficult task. Yet detailed analysis of those sites were not in the scope of the study. Therefore, an approximated network connection MRC was determined as follows:

1. First, the average MRC to connect to the backbone for medium/large facilities (ATCTs, TRACONs, & ARTCCs) in the representative architectures was computed: MRC_{avg-1} . A similar MRC was computed for small/remote facilities (those not ATCTs, TRACONs, or ARTCCs): MRC_{avg-2} .
2. Of the 80 additional facilities not selected for analysis but with a circuit end-point in the baseline circuit list, 30 were classified as medium/large facilities and 50 as small/remote facilities.
3. For the medium/large FAA facility connections, 10% of the cost to connect the facility to the backbone is attributed to the communication to nodes within the selected representative architecture; therefore, additional MRC to account for is $0.10 * 30 \text{ facilities} * MRC_{avg-1}$.
4. For small/remote FAA facility connections, 50% of the cost to connect the facility to the backbone is attributed to communication to nodes within the representative architecture; therefore, additional MRC to account for is $0.50 * 50 \text{ facilities} * MRC_{avg-2}$.

Using this procedure, the incremental MRCs to be accounted for in each of the proposed architecture scenario is summarized in Table 5.4-11.

Table 5.4-11: MRC for Distant End-Point Network Access

Architecture Scenario	MRC_{avg-1}	MRC_{avg-2}	Medium/Large Facility Incremental MRC ($0.1 * 30 * MRC_{avg-1}$)	Small/Remote Facility Incremental MRC ($0.5 * 50 * MRC_{avg-2}$)	Total Incremental MRC
1A	\$6,144	\$600	\$18,432	\$15,000	\$33,432
1B	\$4,575	\$798	\$13,725	\$19,950	\$33,675
2	\$2,747	\$394	\$8,241	\$9,850	\$18,091

5.4.4 Total Circuit MRC for Architecture Scenarios

Based on the calculations in the previous sections, the total circuit MRC for each proposed architecture was computed by summing the circuit MRC values found in Section 5.4.2.2, Section 5.4.2.3, and Section 5.4.2.4 with backbone usage charges and incremental MRC to account for distant circuit end-point connections to the network (for those end-points not in the representative architecture). The total circuit MRC values for the proposed architectures and the baseline architecture are summarized in Table 5.4-12.

Table 5.4-12: Total Circuit MRC for Baseline and Proposed Architectures

Baseline	Scenario 1A	Scenario 1B	Scenario 2
\$231,474	\$163,571	\$140,761	\$95,508

5.4.5 Circuit NRC and CPE Cost Considerations

In addition to the circuit MRC values analyzed above, each of the communication architectures may incur costs associated with new customer premise communication equipment, replacement communication equipment, equipment operation and maintenance charges, and circuit set-up non-recurring charges. As indicated in Section 5.4.1, these costs could not be evaluated for the baseline architecture. These costs, however, have been estimated for the three proposed network architectures and are addressed in the following sections.

5.4.5.1 Circuit Non Recurring Costs

The non-recurring setup and activation charges for the circuits in the proposed architecture scenarios were calculated using the FLAPS and SDP Pricer pricing tools (reference descriptions in Section 5.4.2). It was assumed that all of the circuits in the proposed architectures that were changed in any manner from the baseline architecture would incur new setup charges, as if no circuit had previously existed. In actuality, some of the existing circuits could be reused, but might carry a different mix of FAA services or have changed internal end-points.

For circuit prices using the FLAPS model, 50% of the non-recurring cost as determined by the model were attributed to circuit setup and activation charges and were included in the circuit non recurring costs. The remainder of the NRC is assumed to account for items such as CPE, which is addressed separately in this report. For circuits priced using the SDP Pricer tool, NRC identified as system installation price (SIP) was used in its entirety as NRC for circuit setup and activation. The circuit non-recurring costs associated with the three proposed network architectures are summarized in Table 5.4-13.

Table 5.4-13: Circuit NRC for Proposed Architecture Scenarios

	Network Architecture		
	Scenario 1A	Scenario 1B	Scenario 2
Circuit NRC	\$294,196	\$277,540	\$294,196

5.4.5.2 Customer Premise Equipment Costs

Consideration of components that comprise CPE was based on the description of premises functions as identified in the draft FAA Future Telecommunication Infrastructure (FTI) *System Requirements Document*.⁸⁰ This document identifies premises equipment generally in terms of user-network interface (UNI) functions, transport bundling functions, and access bundling functions.

The UNI functions are used to terminate telecommunication services in the interfaces required by FAA communication service classes at the service delivery point.⁸¹ The UNI functions directly interact with legacy equipment and provide protocol conversion as necessary (analog to digital or voice coding). In the proposed architectures, the UNI function is included in packet-voice gateway equipment (for voice coding/decoding), digital signaling gateway equipment (for digital signaling over voice analog/digital conversion), and UNI Router cards that perform data encapsulation, voice coding/decoding, and analog/digital conversion.

Transport bundling functions are defined in the FTI reference to address instances where several different FAA communication requirements exist between the same FAA locations or between a FAA location and a switched (networked) data service port or POP. In these cases, a cost-effective solution may include the combination of various FAA services on a common transport – or transport bundling. These functions are addressed in the proposed architectures using multiplexing modems, ethernet hubs and LAN modems, ethernet switches, and router data aggregation functions.

Access bundling functions are similar to transport bundling functions, but address the aggregation of network access communications from UNIs and transport bundling equipment onto larger bandwidth access lines. These functions are incorporated into the internal and campus routers defined in the proposed architecture scenarios.

In order to cost specific CPE to address the UNI and bundling functions, a set of primarily COTS communication and network equipment was identified and priced. The set of equipment was selected to satisfy the range of communication requirements encountered in the development of campus area networks and connection of FAA nodes to a commercial backbone network. All routing equipment was defined to be high-end systems with internal redundancy of key functions and components most likely to contribute to faults (i.e. power supplies, cooling fans, etc.) For those communications classified as critical, a complete redundant component assumed to be operated in the hot-standby mode was specified for the campus network. This equipment would be running appropriate software, e.g. Hot Standby Routing Protocol, to minimize the visibility of system faults to end-users and automatically redirect communications around failures. The prices identified for the network equipment are company list price with a typical government discount⁸². Prices identified for key network components used to derive CPE costs are provided in Table 5.4-14.

A tally of all of the network equipment used in the proposed architectures was computed and incorporated into a CPE cost calculation spreadsheet. The CPE identified is applicable to all of the proposed architecture scenarios. Although the equipment associated with the screen-subnet security feature could

be eliminated at non-hub nodes in architecture scenario 1B (if connections are made to the hub campus router and the hub node was designated to provide the screening security feature), the security equipment was included in the architecture to provide a conservative approach and to accommodate migration to other architecture scenarios (system growth). Reference Section 4.5.1 for additional information on the proposed architecture scenarios and Section 2.2.5.2.3 for information on screen-subnet security features.

The CPE cost calculations spreadsheet also includes cost allocations to system spares, installation charges, and site activation charges. Additionally, a CPE operation and maintenance charge was assumed as a yearly fee of 15% of the total equipment cost. The CPE cost spreadsheet is provided in Table 5.4-15.

As indicated in Table 5.4-15 above, the yearly CPE cost accounting for new equipment; installation and testing; spares; equipment integration and activation; and CPE operation and maintenance is approximately \$550,000/year (10 year lifecycle).

Table 5.4-14: Representative Network CPE and Associated Costs

Equipment	List cost/unit	Cost/Unit with Gov't Discount	Comment
Switches and Routers			
High-End Small Campus/External Router - high performance, redundant ps, 3 RS-232 or similar ports, 1 ethernet port, 1 WAN port (DS0 or DS1)	\$5,995	\$2,698	Cisco 2610 Router with IP Software
High-End Small Campus Router - high performance, redundant ps, 3 RS-232 or similar ports, 5 ethernet ports, 1 WAN port (DS0 or DS1)	\$20,600	\$9,270	Cisco 3640 Router with IP Software
High-End Small Internal Router - high performance, redundant ps, 3 RS-232 or similar ports, 5 ethernet ports	\$19,600	\$8,820	Cisco 3640 Router with IP Software
High-End Small External Router - high performance, redundant ps, 2 ethernet ports, 2 WAN ports (DS0 or DS1)	\$5,879	\$2,646	Cisco 2621 Router with IP Software
High-End Medium-size Internal Router - high performance, redundant ps, 8 RS-232 or similar ports, 2 ethernet ports	\$8,979	\$4,041	Cisco 2621 Router with IP Software
High-End Medium-size Campus Router - high performance, redundant ps, 5 RS-232 or similar ports, 8 ethernet ports, 1 WAN interface (DS1 or FT1)	\$24,800	\$11,160	Cisco 3640 Router with IP Software
High-End Medium-size External Router - high performance, redundant ps, 2 ethernet ports, 2 WAN interface (DS1 or FT1)	\$5,879	\$2,646	Cisco 2621 Router with IP Software
High-End Medium-Large External Router - high performance, redundant ps, 2 ethernet ports, 4 WAN interface (DS1)	\$20,700	\$9,315	Cisco 3640 Router with IP Software
High-End Large Internal Router - high performance, redundant ps, 20 RS-232 or similar ports, 5 ethernet ports	\$124,264	\$55,919	Cisco 7513 Router with IP software
High-End Large-size External Router - high performance, redundant ps, 2 ethernet ports, 12 WAN interface ports (DS1)	\$36,700	\$16,515	Cisco 3662 Router with IP Software
Gateway Equipment			
Packet Voice Gateway (VoIP Gateway) - 7 voice ports, 1 ethernet port	\$20,300	\$9,135	VipNet VG622/12
Custom Digital Signaling Gateway (for radio interface) - 10 interface ports, 1 ethernet port	--	\$20,000	Estimated price based on similar custom products
Other Communication Equipment			
Bastion Host Server - Firewall with VPN capability	\$15,300	\$6,885	Net Pathways WatchGuard Firewall (\$7,800) & server network (\$7,500)
Ethernet Switch - Ethernet/Fast Ethernet/Gigabit Ethernet - 10 ports	\$6,775	\$3,049	Asante Technology Intrastack Switch
Ethernet Bridge	\$388	\$175	CNET Technologies CN 4020 ERP
Ethernet Hub	\$60	\$27	3COM Office Connect Ethernet Hub
LAN modem/access device	\$999	\$450	CISCO 805 Access Router/3 COM LAN modem
MUX/DMX CSU/DSU/Modem	--	\$2,150	Codex 3600 series Mux/DMX CSU/DSU/modem

Table 5.4-15: Proposed Architectures CPE Tally and Costs

Customer Premise Equipment	Unit Cost (\$)	Units/Node	Total System Cost
<u>Switches and Routers</u>			
High-End Small Campus/External Router - high performance, redundant ps, 3 RS-232 or similar ports, 1 ethernet port, 1 WAN port (DS0 or DS1)	\$2,698	15	\$40,466
High-End Small Campus Router - high performance, redundant ps, 3 RS-232 or similar ports, 5 ethernet ports, 1 WAN port (DS0 or DS1)	\$9,270	29	\$268,830
High-End Small Internal Router - high performance, redundant ps, 3 RS-232 or similar ports, 5 ethernet ports	\$8,820	8	\$70,560
High-End Small External Router - high performance, redundant ps, 2 ethernet ports, 2 WAN ports (DS0 or DS1)	\$2,646	15	\$39,683
High-End Medium-size Internal Router - high performance, redundant ps, 8 RS-232 or similar ports, 2 ethernet ports	\$4,041	14	\$56,568
High-End Medium-size Campus Router - high performance, redundant ps, 5 RS-232 or similar ports, 8 ethernet ports, 1 WAN interface (DS1 or FT1)	\$11,160	16	\$178,560
High-End Medium-size External Router - high performance, redundant ps, 2 ethernet ports, 2 WAN interface (DS1 or FT1)	\$2,646	8	\$21,164
High-End Medium-Large External Router - high performance, redundant ps, 2 ethernet ports, 4 WAN interface (DS1)	\$9,315	4	\$37,260
High-End Large Internal Router - high performance, redundant ps, 20 RS-232 or similar ports, 5 ethernet ports	\$55,919	7	\$391,432
High-End Large-size External Router - high performance, redundant ps, 2 ethernet ports, 12 WAN interface ports (DS1)	\$16,515	2	\$33,030
<u>Gateway Equipment</u>			
Packet Voice Gateway (VoIP Gateway) - 7 voice ports, 1 ethernet port	\$9,135	84	\$767,340
Custom Digital Signaling Gateway (for radio interface) - 10 interface ports, 1 ethernet port	\$20,000	56	\$1,120,000
		0	\$0
<u>Other Communication Equipment</u>			
Bastion Host Server - Firewall with VPN capability	\$6,885	27	\$185,895
Ethernet Switch - Ethernet/Fast Ethernet/Gigabit Ethernet - 10 ports	\$3,049	13	\$39,634
Ethernet Bridge	\$175	8	\$1,397
Ethernet Hub	\$27	30	\$810
LAN modem/access device	\$450	26	\$11,688
MUX/DMX CSU/DSU/Modem	\$2,150	8	\$17,200
Total New CPE Prime Equipment			\$3,281,517
Installation and Testing (@ 18% of new CPE)			\$590,673
Initial Spares (@ 10% of new CPE)			\$328,152
H/W and S/W Integration and Site Activation (@ 25% of new CPE)			\$820,379
Total New CPE			\$5,020,721
		\$MRC	
Averaged Monthly CPE Operation and Maintenance			\$4,101.90
MRC over life cycle of	10	years	\$492,228
Total Cost in Year 2000 Constant Dollars over a lifecycle of			10 years
			\$5,512,948
Yearly Cost Factoring Uniform Equipment Depreciation (based on Year 2000 Constant Dollars)			\$551,295

5.4.6 Cost Summary

A summary of costs calculated in the study for the baseline and proposed network architectures is presented in Table 5.4-16. This summary provides a one year cost comparison.

Table 5.4-16: Cost Summary

	Baseline Architecture	Network Scenario 1A	Network Scenario 1B	Network Scenario 2
1 Year Circuit Costs	\$2,777,688	\$1,962,852	\$1,689,132	\$1,146,096
Circuit NRC/Activation	Not Assessed	\$294,196	\$277,540	\$294,196
New Replacement CPE (yearly based on 10 year lifecycle)	Not Assessed	\$551,295	\$551,295	\$551,295
Total	Not Assessed	\$2,808,343	\$2,517,967	\$1,991,587

A graphical depiction of the cost summary data is provided in Figure 5.4-5. In this figure, the box with the question mark above the baseline 1-year circuit cost is representative of cost for replacement equipment and circuits that would be required to maintain the current level of communication. This cost was not assessed in this study.

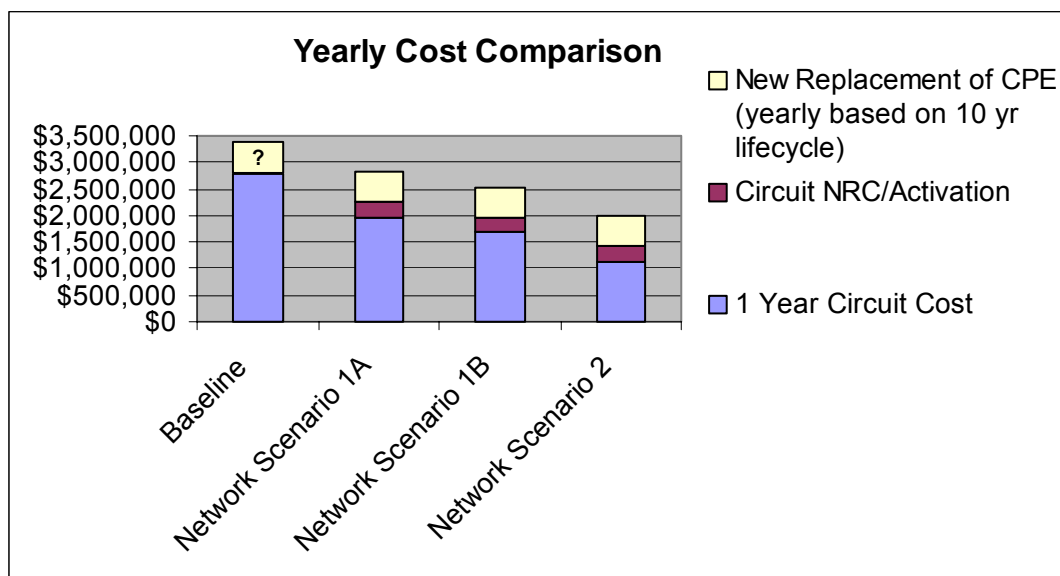


Figure 5.4-5: Cost Summary Data

6. CONCLUSIONS AND RECOMMENDATIONS

6.1 WORK SUMMARY

The primary purpose of the study was to investigate the extent to which the communications requirements of the NAS could be efficiently met by a modern packet communications network. This investigation addressed a number of issues including:

- Meeting NAS requirements for Quality of Service (QoS) in the shared resource environment of a packet network: the primary QoS parameters considered were bandwidth, availability, and data latency.
- Meeting FAA security requirements within a relatively open (compared with current point-to-point communications) packet network.
- Potential for reduction in telecommunications costs.
- The capability of enterprise management tools for monitoring the communications network, and for managing the NAS applications, application data and other NAS resources.

The assessment of satisfying NAS communications requirements within the framework of a modern packet network was done at both a general level and a detailed level:

- At a general level, in Section 2 we summarized the applicable technologies for modern communications networks, and in Section 3 we discussed the application of these to the NAS requirements.
- At a detailed level, in Section 4 we developed alternative communications network designs that support a major subset of the NAS facilities in the Cleveland ARTCC, and in Section 5 we evaluated the alternatives with respect to performance versus requirements and cost.

6.2 CONCLUSIONS

Assessments at both the general and detailed levels indicate that the NAS communications requirements can be met. The following general conclusions with respect to NAS can be made:

- **NAS needs for bandwidth:** existing and envisioned commercial communications networks have adequate bandwidth to carry the NAS data traffic. In recent years, there has been a huge growth in data communications networks and in the high data rate services on such networks. NAS needs for bandwidth (now and in the future) are easily met by commercial network services.
- **NAS needs for high availability (>0.99999):** where NAS facilities such as ARTCCs and large TRACONS are in proximity to the Points-of-Presence (POPs) of a communications network, NAS needs for such high availability can be met with current and envisioned service offerings. Current service providers achieve availabilities of 99.999% to 100% over their modern networks with technologies that incorporate “built-in” redundancy and self-healing. For small and remote NAS facilities that require long distance access lines to networks, the 0.99999 availability requirement

can only be met by incorporating redundancy in the access lines. However, with the emergence of new wired and wireless access technologies, the FAA has many more cost-effective options for incorporating redundancy for access lines from small and remote NAS facilities.

- **NAS need for low data latency:** although the data latency for a packet network will typically be higher than for point-to-point communications, packet communications networks achieve well under the 300 msec maximum allowed for communications latency for critical radar data. For voice carried over a packet network, the end-to-end latency goals are in the range of 250 msec to 300 msec, but only 150 msec or less may be allocated to the communications. Meeting a 150 msec latency for packet voice is readily achievable, but, where the latency allocation to the communications network is much below 150 msec, advancements over the current practice will be required.
- **NAS needs for security:** security is a big issue for all corporations and institutions that use packet networks and, as a result, a wealth of alternative standards, technologies, and products that will provide adequate security are available for the NAS. However, implementation of a security architecture can lead to increased data latency and a large increase in processing burden at NAS facilities so it is important that these constraints are recognized in the implementation of NAS security.
- **NAS needs for enterprise management:** enterprise management also is a big issue for all corporations and institutions that use packet networks, and as a result, there are a wealth of standards, technologies, and products that are available to the NAS. Enterprise management is clearly a needed element for efficient operation of the NAS, and includes such areas as real-time network monitoring, network configuration management, management of the IP address space, and overall management of the FAA services and application data that those services are based on.

For the detailed assessment, alternative communications network architectures for the Cleveland ARTCC were developed around three alternative Scenarios pictured in Figure 6.2-1. These three scenarios are as follows:

- **Scenario 1A**
 - Assumes a low density of network POPs, comparable to the density of POPs that exists today.
 - Connects all NAS facilities to the nearest network POP; in the case of small and remote NAS facilities, some of the access lines span large distances.
- **Scenario 1B**
 - Assumes a low density of network POPs, comparable to the density of POPs that exists today.
 - Connects large NAS facilities to the nearest network POP.
 - Connects small and remote NAS facilities to the nearest large NAS facility.
- **Scenario 2**
 - Assumes a high density of network POPs, comparable to the density of POPs that is projected to exist in the future; this projection was based upon the current density of ISP points-of-presence (which is quite dense).

- Connects all NAS facilities to the nearest network POP; with the dense POP assumption, even in the case of small and remote NAS facilities tend to be close to a network POP.

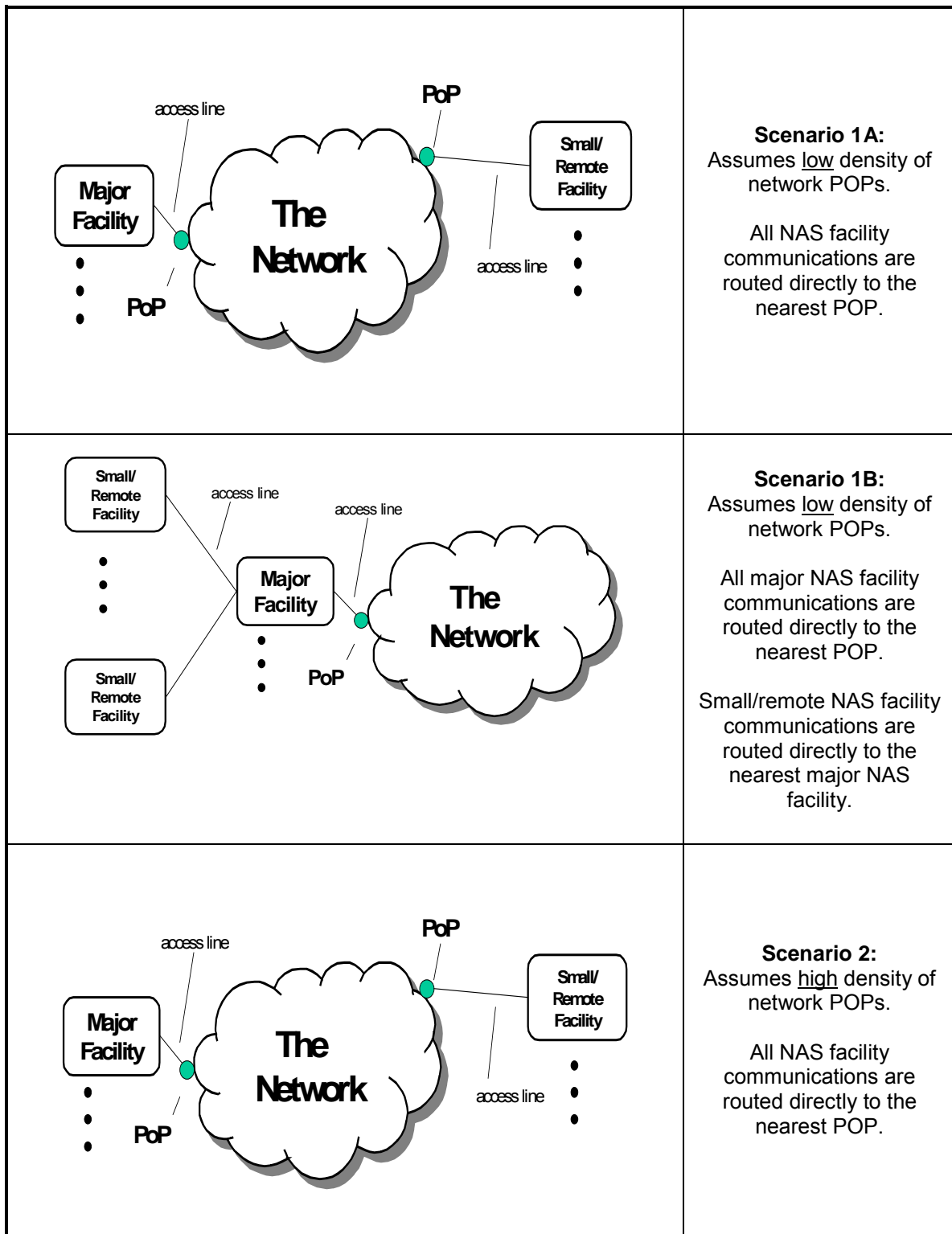
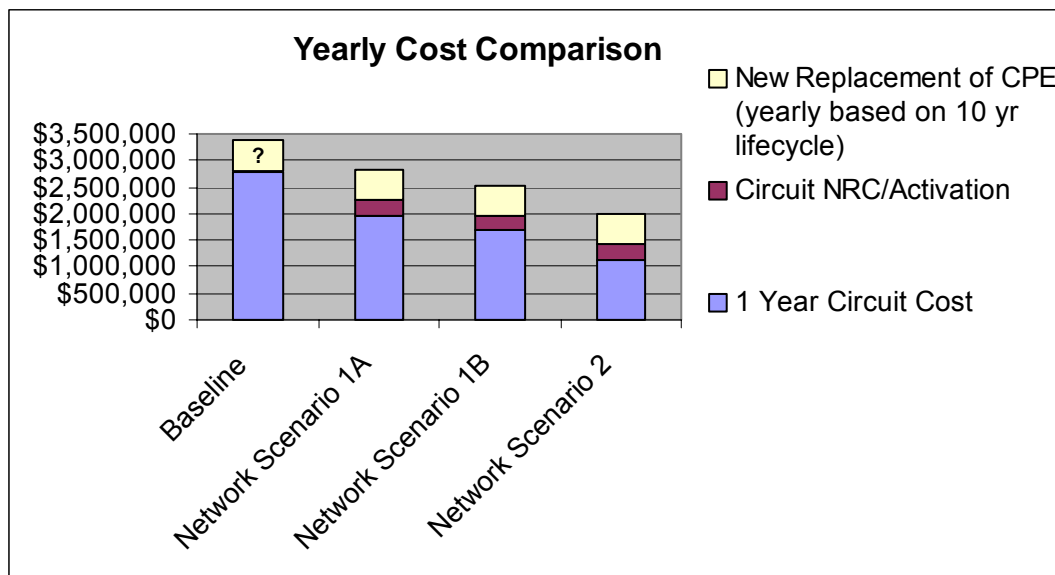


Figure 6.2-1: Alternative Architectures Considered

A detailed cost estimate of the leased lines required was made for each of these scenarios and compared to the baseline of current NAS communications. The detailed methodology is described in Section 5. Figure 6.2-2 summarizes these estimates. Note that cost savings are estimated for all the alternatives considered.



Note: Cost for replacement of circuits and equipment for the baseline architecture was not addressed in this study.

Figure 6.2-2: Monthly Cost of Leased Lines for Baseline and Alternatives

6.3 RECOMMENDATIONS

The FAA should pursue a NAS communications architecture in accord with Scenario 1B above. The rationale is as follows:

- Highly reliable network communications between facilities near network POPs is a mature service that meets FAA needs. Such a network can provide 99.999% to 100% availability of communications between major NAS facilities.
- Maintaining point-to-point links between small/remote facilities and major NAS facilities, for packet communications, is a positive incremental step that affords virtually all the information sharing possible in a packet network, while it has less implementation risks and presents less of a security challenge than Scenario 1A and Scenario 2.

The FAA should take a uniform and comprehensive approach in application of enterprise management technology and tools to the NAS. In addition to monitoring and control of communications an application network elements, enterprise management incorporates IP address management, implementation of a domain naming system and servers, directory structures and data warehousing.

In this study, a number of FAA facilities were identified in which different programs in the same location had complete separate communications. Although we did not analyze the economics of doing so, we believe that there may be great advantage (lower leased communications costs) in implementing “campus area networks” that aggregate data from multiple programs and can share a common access communications to the network.

In summation, we recommend that FAA migrate toward treating communications and the supporting functions of security and enterprise management as common utilities that provide constant and uniform support across all FAA services, because this will enable FAA to focus on its primary mission, which is the provision of air traffic control and related services.

LIST OF ABBREVIATIONS, ACRONYMS AND CODES

NOTE: There are several types of codes that are used in Section 4, Section 5, and in Appendix B of this document. The most common codes found throughout the document are Service Codes (SVC), Program Designator Codes (PDC), Facility (FAC), and Location Identifiers (LID). These codes are used to differentiate the endpoints and purposes of leased lines in the TIMS database, and are defined in the *Current FAA Telecommunications System and Facility Description Manual*. The Service Code is a three or four alpha-character code used to identify the services being provided by a system or its interconnecting telecommunications. PDCs are unique two alpha-character codes assigned to each program using telecommunications services, and are a fiscal management tool used to allocate and monitor the costs of circuits or equipment associated with each program. The FAC code is used to differentiate telecommunications service locations. Facility types are identified using abbreviations unique to each facility. The LID is used to identify specific geographical locations.

Both the FAA official Location Identifier document, FAA 7350.6 and the TIMS database use all capital letters for location identifiers and codes. For consistency, that convention has been followed in this listing when presenting Location Identifiers and the location they refer to.

TERM	Definition
0G6	WILLIAMS COUNTY AIRPORT, BRYAN, OH
10BASE-T	10 Mbps twisted pair Ethernet
14G	FREMONT, OH, AIRPORT
1D2	PLYMOUTH, MI, AIRPORT
1G3	KENT STATE UNIVERSITY AIRPORT, KENT, OH.
1G5	MEDINA, OH, MUNICIPAL AIRPORT
22G	LORAIN/ELYRIA, OH, COUNTY AIRPORT
22V	CHENOWITH AIRPORT, LAST CHANCE, CO
2G6	PORT MEADVILLE AIRPORT, MEADVILLE, PA
2G7	NEW CASTLE, PA, MUNICIPAL AIRPORT
38KY	WILLIAMSTOWN, KY, ATOVN
3DES	Triple Digital Encryption Standard
3G	Third Generation
3HE	LIVINGSTON COUNTY AIRPORT, HOWELL, MI,
4F-BLSR	4-Fiber Bi-directional Line Switch Ring
4G1	GREENVILLE, PA, MUNICIPAL AIRPORT
4I3	FAA RTR facility in Mt. Vernon, OH
5G7	BLUFFTON, OH, AIRPORT
7G2	ASHTABULA COUNTY, OH, AIRPORT
9G0	BUFFALO, NY, AIRFIELD AIRPORT
A/G	Air/Ground
AA	TMS (central flow) voice circuits
AB	Inter-ARTCC circuits used for critical ATC/hand-off information
ABI	Crash Fire Rescue Bldg Abilene, TX, Municipal Airport
ABR	Available Bit Rate
AC	ARTCC to non-ARTCC (not ARTCCs to AFSSs) used for hand-off/air traffic control

TERM	Definition
AC	Alternating Current
ACC	Area Control Center
ACCC	Area Control Computer Complex
ACCOUN	Account
ACELP	Adaptive Code-Excited Linear Prediction
ACK	Nantucket Memorial Airport Fire/Crash Station, Nantucket, MA
ACKS	Acknowledgements
ACO	Aircraft Certification Office or AKRON, OH, VOR/DME
ACY	ATLANTIC CITY, NJ, INTERNATIONAL AIRPORT, VORTAC
ACYB	FAATC HANGAR, ATLANTIC CITY, NJ
ADAS	AWOS Data Acquisition System
ADDA	Administrative Data
ADG	LENAWEE COUNTY AIRPORT, ADRIAN, MI
ADIN	AUTODIN Service
ADO	FAA Airport District Office
ADPCM	Adaptive Differential Pulse Code Modulation
ADS	ADDISON AIRPORT, ILS/DME, DALLAS-ADDISON, TX
ADS-B	Automatic Dependent Surveillance Broadcast (VDL Mode 4)
ADSL	Asymmetric Digital Subscriber Line
ADSY	Administrative voice switches.
ADTN	Administrative Data Transmission Network
ADTNC	ADTN 2000 Network Control Center
ADVO	Administrative Voice Service
ADW	ANDREWS AIR FORCE BASE, BASEOPS, VORTAC, CAMP SPRINGS, MD
AE	Interphone circuits (not ARTCCs) critical to interfacility communications
AES	Advanced Encryption Standard
AF	Flight assistance private line circuits
AFB	Air Force Base
AFJ	WASHINGTON, PA, COUNTY AIRPORT, LOC/DME
AFS	Airway Facilities Sector Office
AFSFO	Airway Facilities Sector Field Office
AFSFU	Airways Facilities Sector Field Unit
AFSOU	Airway Facilities Sector Field Office Unit
AFSS	Automated Flight Service Station
AFTN	Aeronautical Fixed Telecommunications Network
AG8	ROMULUS, MI, RCLR
AGC	ALLEGHENY COUNTY, PA, AIRPORT, ILS, ALLEGHENY VORTAC
AGL	Great Lakes Regional Office
AH	Authentication Header
AH8	ANN ARBOR, MI, RCLR
AIS	Aeronautical Information System
AKR	FULTON INTERNATIONAL AIRPORT, LOC/DME, AKRON, OH
ALS	Approach Lighting System
ALSF2	ALS with Sequenced Flashers II
AM	Miscellaneous interphone circuits
AM	Amplitude Modulation
AMC	FAA Internet Access point in Oklahoma City, Oklahoma
AMN	ALMA, MI, RTR
ANGB	Air National Guard Base
ANICS	Alaska NAS Interfacility Communications System
ANSI	American National Standards Institute

TERM	Definition
AOC	Airline Operational Control
AOH	ALLEN COUNTY AIRPORT, ILS, VOR, LIMA, OH
AOO	ALTOONA, PA, AFSS, VOR, ALTOONA-BLAIR COUNTY AIRPORT, ILS
AOP	ANTELOPE NDB, ROCK SPRINGS, WY
AOP	NAS Operations Organization
APB	Acquisition Program Baseline
APE	APPLETON, OH, VORTAC
API	Application Programming Interface
APN	ALPENA, MI, COUNTY AIRPORT, BASEOPS, ILS, VORTAC
APNIC	Asia Pacific Network Information Centre
APPN	Advanced Peer to Peer Networking, a distributed networking feature of IBM's System Network Architecture
AR	ARTCC to non-ARTCC circuits not used for hand-off/air traffic control
ARB	ANN ARBOR, MI, MUNICIPAL AIRPORT
ARCTR	FAA Aeronautical Center
ARIN	American Registry for Internet Numbers
ARINC	Aeronautical Radio, Inc.
ARMS	Airport Remote Monitoring System
ARPT	Airport
ARSR	Air Route Surveillance Radar
ARSR-4	ARSR model 4
ARSR-9	ARSR model 9
ARTCC	Air Route Traffic Control Center
ARTS	Automated Radar Terminal System
AS	Non-critical interphone circuits (excludes ARTCCs)
ASC	AUTODIN Switching Center
ASD	FAA Systems Engineering Organization
ASD	Aircraft Situation Display
ASD-400	The FAA's Investment Analysis and Operations Research Directorate
ASDE	Airport Surface Detection Equipment
ASOS	Automated Surface Observing Station
ASR	Airport Surveillance Radar
AT	Air Traffic or Air Taxi
ATC	Air Traffic Control
ATCBI	Air Traffic Control Beacon Indicator
ATCBR	Air Traffic Control Beacon Radar
ATCP	Air Traffic Control Position
ATCRB	Air Traffic Control Radar Beacon
ATCSCC	Air Traffic Control System Command Center
ATCT	Airport Traffic Control Tower
ATIS	Automated Terminal Information Service
ATL	ATLANTA, GA, NADIN CENTER, THE WILLIAM B HARTSFIELD ATLANTA INTERNATIONAL AIRPORT, ILS/DME,
ATM	Air Traffic Management
ATM	Asynchronous Transfer Mode
ATN	Aeronautical Telecommunications Network
ATOVN	AUTOVON Network
ATS	Air Traffic Service
AUTODIN	DOD AUTOMATIC Digital Interface Network
AUTOVON	AUTOMATIC VOICE Network, the DOD worldwide switched network system
avg	Average
AVON	AUTOVON Service

TERM	Definition
AVP	WILKES-BARRE-SCRANTON, PA, INTERNATIONAL AIRPORT, ILS/DME
AWA	FAA Internet Access point in Washington, DC
AWG	American Wire Gauge, the US standard for non-ferrous conductors
AWIS	Airport Weather Information System
AWOS	Automated Weather Observing Station
AWP	Aviation Weather Processor
AWP	FAA Internet Access point in Los Angeles, California
AZO	KALAMAZOO/BATTLE CREEK INTERNATIONAL AIRPORT
B channel	Bearer channel
BA	High speed data circuits, SVCA and SVCB
BASOP	Base Operations
BAX	BAD AXE, MI, HURON COUNTY MEMORIAL AIRPORT, VOR/DME
BB	Service "A" TTY circuits and/or associated equipment
BCN	Back Up Communication Network
BDAT	Digitized Beacon Data
BER	Bit Error Rate
BF	FDIO data circuits
BFD	BRADFORD, PA, REGIONAL AIRPORT
BGM	BINGHAMTON, NY, REGIONAL AIRPORT, VORTAC, ILS
BI	FSDPS Model 1A (AFSS/ARTCC) data circuits and/or associated equipment
BI-5	Beacon Interrogator model 5
BJ	FSDPS Model 1 Full Capacity (AFSS/ARTCC) data circuits
BJJ	WAYNE COUNTY AIRPORT, WOOSTER, OH
BK	AFTN circuits
BKL	BURKE LAKEFRONT AIRPORT, CLEVELAND, OH
BLSR	Bi-directional Line Switch Ring
BM8	CENTERVILLE, OH, RCAG
BOS	GENERAL EDWARD LAWRENCE LOGAN INTERNATIONAL AIRPORT, ILS/DME, VORTAC
bps	Bits per second
BR	ATC computer circuits, ARTCC to ATCT/TRACO
BRI	Basic Rate Interface
BTP	BUTLER COUNTY/K. W. SCHOLTER FIELD AIRPORT, BUTLER, PA,
BU	Dedicated weather network circuits (WCP, RWP, WMSCR, WMP, WARP) or Back Up when combined with a service, such as RDAT-BU
BUEC	Back Up Emergency Communications
BUF	GREATER BUFFALO, NY, INTERNATIONAL AIRPORT, VORTAC, AFSS
BUFA	BUFFALO, NY, REIL, WSCMO, WSFO
BVI	BEAVER COUNTY AIRPORT, LOC, BEAVER FALLS, PA
BW	AWIS data circuits or Bandwidth
BWM	Band Width Manager
BX	Weather service facilities (WSO, WSFO) data circuits
BY	Critical TMS (central flow) data circuits
CA	RCAG primary circuits
CA	Certificate Authority
CA	California
CAC	Connection (or Call) Admission Control
CACI	An international information technology products and services company
CAK	AKRON-CANTON, OH, REGIONAL AIRPORT
CASFO	Civil Aviation Security Field Office
CASFU	Civil Aviation Security Field Unit

TERM	Definition
CB	RCAG backup circuits
CBE	GREATER CUMBERLAND, MD, REGIONAL AIRPORT, LOC/DME
CBI	Computer Based Instruction
CBR	Constant Bit Rate
CC	RCAG circuits physically and electrically diverse for same frequency/airspace
CCCH	Central Computer Complex Host
CCITT	Consultative Committee on International Telephony and Telegraphy
CCSD	Command Communications System Designator
ccTLD	County Code Top Level Domain
CD	Common Digitizer
CDV	Cell Delay Variation
CDVT	Cell Delay Variation Tolerance
CE	BUEC circuits
CELP	Code-Excited Linear Prediction
CENTREX	Switching equipment located in the Local Exchange Carrier's switching office
CERAP	Combined Center/ Radar Approach Control
CFB	BINGHAMTON, NY, VORTAC
CFCF	Central Flow Control Facility
CFCS	Central Flow Control Service
CFWSU	Central Flow Weather Service Unit
CGF	CAYAHOGA COUNTY AIRPORT, ILS/DME, CLEVELAND, OH
CH	Flight Service Station RCO circuits
CHAP	Challenge Handshake Authentication Protocol
CIP	CLARION, PA, VORTAC
CIP	Capital Investment Plan
CIR	Committed Information Rate
CISCO	Cisco Systems, Inc., a company that sells information networks products and services
CJ	EFAS circuits
CK	HI-EFAS circuits
CKB	BENEDUM AIRPORT, CLARKSBURG, WV
CL	Cell Loss Ratio
CLE	CLEVELAND, OH, AFSS, ILS, HOPKINS INTERNATIONAL AIRPORT
CLR	Cell Loss Rate
CMH	PORT COLUMBUS INTERNATIONAL AIRPORT, ILS/DME, WSO
CMHB	COLUMBUS, OH, RCO
CN	Air/Ground broadcast of recorded messages from terminal facilities
CNSI	Common Network Security Interface
CNSM	Common Network Security Model
CO	A/G broadcasts of recorded messages from FSS facilities (HIWAS, TWEB)
COMCO	Command Communications Outlet
COMMAND_CO	Command Communications System Designator code
CONUS	Continental, Contiguous or Conterminous United States
CORP	Private Corporation
COS	CITY OF COLORADO SPRINGS, CO, MUNICIPAL AIRPORT, BASEOPS, ILS, COLORADO SPRINGS VORTAC
CoS	Class of Service
COTS	Commercial Off-The-Shelf
CPE	Customer Premise Equipment
CPQ	CAPITAL CITY ILS, LANSING MI
CPU	Central Processing Unit
CPV	COOPERSVILLE, MI, ARSR

TERM	Definition
CRC	Cyclic Redundancy Check
CRI	CANARSIE, NY, VOR/DME
CRL	CARLETON, MI, VORTAC
CS	ARINC Air to Ground Voice
CSA_ACCOUN	Communications Service Authorization number
CS-ACELP	Conjugate Structure ACELP
CSPP	COTS Security Protection Profile
CSU	Channel Service Unit
CT	Terminal RTR circuits
CTAS	Center/TRACON Automation System
CTL	Control
CW	Continuous Wave
CWSU	Central Weather Service Unit
CXR	CHARDON, OH, VORTAC
D channel	Data channel
DA	Direct Access
DAP	Directory Access Protocol
DARC	Direct Access Radar Channel
DARPA	Defense Advanced Research Projects Agency
DAV	Data Above Voice
DAY	DAYTON, OH, AFSS
Db	Decibel
dBm	Decibels below 1 milliwatt
DBRITE	Digital Bright Radar Indicator Tower Equipment
DC	Terminal primary radar (Primary Path)
DC	District of Columbia
DCC	CENTRAL FLOW CONTROL, HERNDON, VA
DCE	Data Communications Equipment
DCP	Data Collection Package
DCX	Abbreviation for the statistical multiplexer in the DMN program
DDC	Direct Department Calling
DDC	Direct Digital Connectivity
DDS	Digital Data Service or System
DES	Data Encryption Standard
DES-CBC	Digital Encryption Standard - Cipher Block Chaining
DET	DETROIT, MI, CITY AIRPORT
DET-1	Designation for the node comprising of the DET IBP
DET-2	Designation for the node comprising the facilities at the Detroit Metro Airport
DETA	DETROIT, MI, RTR
DF	Direction Finder
DFI	DEFIANCE, OH, MEMORIAL AIRPORT
DHCP	Dynamic Host Configuration Protocol
DiffServ	Differentiated Services
DIRF	Direction Finder
DIRMM	Departmental Information Resources Management Manual
DISA	Defense Information Systems Agency
DITCO	Defense Information Technology Contracting Organization
DJ	Backup narrowband radar circuits
DJB	Designator for the node comprising FAA radio and weather facilities at the Lorain County Airport
DJM	Dual Jack Module
DKK	CHATAUQUA COUNTY/DUNKIRK, NY, AIRPORT, VORTAC

TERM	Definition
DLAP	Data Link Application Processor
DLP	Data Link Processor
DME	Distance Measuring Equipment
DMI	FAA Navigation Facilities (LOM, OM, LOC, GS) in Romulus and South Gate, MI
DMN	Data Multiplexing Network
DMZ	De-Militarized Zone
DNS	Domain Naming System
DNY	DELANCEY, NY, VOR/DME
DoC	Department of Commerce
DoD	Department of Defense
DOD	Department of Defense
DOT	Department of Transportation
DQN	DAYTON, OH, VOR/DME
DR	Remote terminal radar circuits (TML, DBRITE, RTAD, etc.)
DS	Digital Signaling
DS3	Digital Signal Level 3 – 44.736 Mbps
DSA	Digital Signal Algorithm
DSB-AM	Double Side Band - Amplitude Modulation
DSL	Digital Subscriber Line
DSN	Defense Switched Network
DSR	Display System Replacement
DSU	Data Service Unit
DSV	DANSVILLE, NY, MUNICIPAL AIRPORT
DTMF	Dual Tone Multi-Frequency
DTW	DETROIT METROPOLITAN WAYNE COUNTY, MI, AIRPORT, ROMULUS, MI
DTW/HUU	Designation for the FAA node comprising facilities in and near the Detroit Metro/Wayne County International Airport
DTWA	ROMULUS, MI, ARSR, RTR, RVR
DTWB	ROMULUS, MI, RCAG
DTWC	NORTHVILLE, MI, ASR
DTWF	DETROIT, MI, RTR
DTWJ	ROMULUS, MI, RTR
DUA	Directory User Agent
DUJ	DU BOIS, PA, FSS, DUBOIS-JEFFERSON COUNTY AIRPORT, ILS
DVC	DBRITE Video Compression
DWC	DETROIT, MI, METROPOLITAN WAYNE COUNTY ILS/DME
DWDM	Dense Wavelength Division Multiplexing
DX	Duplex
DXO	DETROIT, MI, VOR/DME
E&M	Ear and Mouth
E1	The European designator for digital signal level 1, operating at a signaling rate of 2.048 Mbps, and capable of handling 32 (thirty-two) 64 Kbps digital channels. The North American equivalent is T1.
E2	Data signal that carries four multiplexed E1 signals at a rate of 8.448 Mbps
E3	Data signal that carries 16 multiplexed E1 signals at a rate of 34.368 Mbps
E4	Data signal that carries four E3 channels, up to 1,920 simultaneous voice conversations at a rate of 139.264 Mbps.
EC	ICSS Type III (AFSS) operational equipment
ECK	PECK, MI, VORTAC
ECOM	En Route Communications: radio communications between the ARTCC and in-

TERM	Definition
	flight aircraft.
EDI	Electronic Data Interface
EE	Interphone key equipment at ATCT (excluding ICSS)
EFAS	En Route Flight Advisory Service
EIA	Electronic Industries Association
EJR	DETROIT, MI, METROPOLITAN WAYNE COUNTY ILS
EKN	ELKINS AFSS, ELKINS-RANDOLPH COUNTY-JENNINGS RANDOLPH FIELD AIRPORT, ELKINS, WV
ELM	ELMIRA, NY, /CORNING REGIONAL AIRPORT, FSS, VOR/DME
ELMC	ELMIRA, NY, RCO
ELX	KEELER, MI, VORTAC
ELZ	WELLSVILLE, NY, MUNICIPAL AIRPORT, VORTAC
ENAV	En Route Navigational Aids
ENET	Enterprise Network Program
ENOC	Enterprise Network Operations Control Center
EPA	FAA LOC and GS facilities in Romulus, M
ERI	ERIE, PA, INTERNATIONAL AIRPORT
ERMS	Environmental Remote Monitoring System
ESP	Encapsulation Payload
ETMS	Enhanced Traffic Management System
ETN	Electronic Tandem Network
ETVS	Enhanced Tower Voice Switch
EVCS	Emergency Voice Communications System
FAA	Federal Aviation Administration
FAATC	FAA Technical Center
FAATSAT	FAA Telecommunications Satellite
FAC	Facility
FB	NAVAID monitor and control circuits without voice for VOR/TACAN/DME etc. or Washington Headquarters when used as TMS TELECOM_OF code
FC	ILS terminal NAVAID circuits
FCOM	FSS Radio Voice Communications
FCPU	Facility Central Processing Unit
FD	Circuits used for NAVAID monitoring and simultaneous air/ground voice transmissions
FDAT	Flight Data Service
FDDI	Fiber Distributed-Data Interface
FDIO	Flight Data Input/Output system
FDY	FINDLAY, OH, AIRPORT
FE	MLS terminal NAVAID circuits or Eastern region when used as TMS TELECOM_OF code
FEDSIM	Federal Systems Integration Center
FFAC	From Facility code
FI	Critical remote weather measuring circuits for RVR and LLWAS
FIFO	First-In-First-Out
FKL	VENANGO REGIONAL AIRPORT, ILS, FRANKLIN, PA; FRANKLIN VORTAC
FL	Visual NAVAIDs and airport lighting circuits (VASI, REIL, etc.) or Great Lakes region when used as TMS TELECOM_OF code
FLAPS	FAA LINCS Pricing Tool
FLID	From Location Identifier code
FM	Fan Marker or New England region when used as TMS TELECOM_OF code
FMH	OTIS ANGB AIRPORT, BASEOPS, ILS/DME, FALMOUTH, MA; OTIS

TERM	Definition
	TACAN
FNT	BISHOP INTERNATIONAL AIRPORT, VORTAC, FLINT, MI
FR	LORAN C circuits
FRAD	Frame Relay Access Device
FSCA	Full Services Access Networks Consortium
FSDO	Flight Standards District Office
FSDPS	Flight Service Data Processing System
FSK	Frequency Shift Keying
FSS	Flight Service Station
FSSA	Flight Service Station Automated Service
FSSP	Flight Service Specialist Position
FSYS	Flight Advisory Equipment System
FT	Non-ILS/Non-MLS terminal NAVAID circuits
FTI	FAA Telecommunications Initiative
FTP	File Transport Protocol
FTS	Federal Telecommunications System 2000
FTS2000	Federal Telecommunications System 2000
FTTB	Fiber To The Building
FTTC	Fiber To The Curb
FTTH	Fiber To The Home
FTZ	FORISTELL, MO, VORTAC
FWA	FORT WAYNE, IN, INTERNATIONAL AIRPORT, BASE OPS, ILS, VORTAC
FXO	Foreign Exchange Office Signaling
FXS	Foreign Exchange Station Signaling
FY	Fiscal Year
G/G	Ground-to-Ground
G114	ITU-T's General Recommendations on the Transmission Quality for an Entire International Telephone Connection
GAS	GALLIA-MEIGS REGIONAL AIRPORT, GALLIOPOLIS, OH
GBI	GREATER BUFFALO, NY, INTERNATIONAL ILS
Gbps	Gigabits per second
GCS	Geostationary Communications
GEE	GENESEO, NY, VOR/DME
GFE	Government-Furnished Equipment
GGT	GEORGETOWN, NY, VORTAC
GIJ	GIPPER VORTAC, NILES, MI
GKJ	PORT MEADVILLE AIRPORT, LOC, MEADVILLE, PA
GLR	OTSEGO COUNTY AIRPORT, ILS, GAYLORD, MI, GAYLORD VOR/DME
GNAS	General NAS Sector Office
GNI	Ground Network Interface
GOES	Geostationary Operational Environment Satellite
GOEST	GOES Terminal
GPS	Global Positioning System
GQQ	GALION, OH, MUNICIPAL AIRPORT
GRB	GREEN BAY, WI, AFSS
GRE	Generic Routing Encapsulation
GRIM	GRIM Corporation Equipment
GRR	KENT COUNTY INTERNATIONAL AIRPORT, ILS, GRAND RAPIDS VOR/DME, GRAND RAPIDS, MI
GS	Glide Slope
GSM	Global System for Mobile Communications

TERM	Definition
GVQ	GENESEE COUNTY ILS, BATAVIA, NY
GW	Gateway
Gxx	ITU-T's series G, recommendations for standards for transmission systems and media, digital systems and networks
H.323	An ITU-T suite of audio, video and application sharing standards applicable to IP Telephony
HC8	PARIS, OH, RCAG
HCAP	High Capacity Carriers
HCS	Host Computer System
HDLC	High-Level Data Link Control protocol
HDQ	Regional or National FAA Headquarters
HDQOU	Airway Facilities Sector Field Office Unit
HLG	WHEELING COUNTY, WV, AIRPORT, VORTAC
HNK	HANCOCK, NY, VORTAC
HOC	HIGHLAND COUNTY, AIRPORT, HILLSBORO, OH
HOC SR	Host Operational Computer System Replacement
HQ	Headquarters
HSRP	Hot Standby Routing Protocol
HTTP	Hypertext Transfer Protocol
HUU	DETROIT METROPOLITAN WAYNE COUNTY ILS, DETROIT, MI,
HUUA	ROMULUS, MI, RVR
HUUB	ROMULUS, MI, RVR
HWCI	HardWare Configuration Item
Hz	Hertz
IA	Administrative services for ATC facilities, business line (exchange service) circuits
IAG	NIAGARA FALLS, NY, INTERNATIONAL AIRPORT, TACAN, ILS
IANA	Internet Assigned Numbers Authority
IAT	Investment Analysis Team
IB	Administrative services for AF facilities, business line (exchange service) circuits
IBP	International Border Point
IC	Administrative services for ATC/AF facilities, business line (exchange service) circuits
ICANN	Internet Corporation for Assigned Names and Numbers
ICEMAN	Integrated Computing Environment - Mainframe and Network
ICSS	Integrated Communications Switching System
ID	Administrative data circuits or Identification
ID	Identifier
IDAT	Interfacility Data Service: Data exchange between air traffic control computers with one end being the ARTCC central computer complex.
IDC	International Data Corporation
IDEA	International Data Encryption Algorithm
IDF	Intermediate Distribution Frame
IETF	Internet Engineering Task Force
IFR	Instrument Flight Rules
IGRP	Inter-Gateway Routing Protocol
IHD	INDIAN HEAD VORTAC, SEVEN SPRINGS, PA
II	Computer Based Instruction (CBI) circuits
IISN	Integrated Interfacility Services Network
IKE	Internet Key Exchange
IL	FM Network - circuit terminating at regional AF repeater link equipment

TERM	Definition
ILE	Killeen Municipal Airport FIRE facility Killeen, TX
ILS	Instrument Landing System
IM	Inner Marker
IMTC	International Multimedia Teleconferencing Consortium
IntServ	Integrated Services
INWATS	INward Wide Area Telephone Service
IO	ADTN 2000 Telecommunications Services
IOS	Cisco's Internet Operating System, used in a majority of Internet routers
IP	Direct charge back to NISC Video Teleconferencing
IP	Internet Protocol
IPDC	IP Device Control
IPsec	A secure version of the Internet Protocol
IPT	WILLIAMSPORT, PA, AFSS, ILS, VORTAC;LYCOMING COUNTY AIRPORT
IPv4	Internet Protocol Specification Version 4
IPv6	Internet Protocol Specification Version 6
IPX	Internet Packet Exchange protocol
IR	Distance Learning FTS 2000 circuits
IRD	Interface Requirements Document
IS	FTS 2000 ISDN Video Conferencing Network
ISAKMP	Internet Security Association and Key Management Protocol
ISDN	Integrated Services Digital Network
ISO	International Standards Organization
ISP	Internet Service Provider
ISS	Information Systems Security
ITH	ITHACA, NY, ILS, VOR/DME, TOMPKINS COUNTY AIRPORT
ITSP	IP Telephony Service Provider
ITU	International Telecommunication Union
ITU-T	International Telecommunication Union (ITU) Transmission Systems and Media
ITWS	Integrated Terminal Weather System
JHW	CHATAQUA COUNTY/JAMESTOWN, NY, AIRPORT, ILS, VOR/DME
JST	JOHNSTOWN- CAMBRIA COUNTY, PA, AIRPORT, ILS, VORTAC
JXN	JACKSON COUNTY, MI,-REYNOLDS FIELD AIRPORT, ILS, VOR/DME
kb/s	Kilobits per second
Kbps	Kilobits per second
kpbs	Kilobits per second
KG-84	An encryption device
km	kilometers
KT	Voice Telecommunications System (VTS)
L2	Layer 2
L2F	Layer 2 Forwarding Protocol in the Virtual Private Network service architecture
L2TP	Layer 2 Tunneling Protocol in the Virtual Private Network service architecture
LAAS	Local Area Augmentation System
LABS	Leased A/B Service: Digital replacement for SVCA and SVCB.
LABSW	LABS Switch System at Anchorage (ALASCOM)
LAN	LANSING, MI, AFSS, ILS, VORTAC, CAPITAL CITY AIRPORT
LAN	Local Area Network
LBE	WESTMORELAND COUNTY AIRPORT, ILS, LATROBE, PA
LCN	Local Communications Network
LDAP	Lightweight Directory Access Protocol
LD-CELP	Low-Delay Code Excited Linear Prediction

TERM	Definition
LDRCL	Low Density Radio Communications Link
LEC	Local Exchange Carrier
LFD	LITCHFIELD, MI, VORTAC
LI	Leap Warning Indicator
LID	Location Identifier
LINCS	Leased Interfacility NAS Communications System
LMDS	Local Multipoint Distribution Service
LNN	LOST NATION MUNICIPAL AIRPORT, VOR/DME, WILLOUGHBY, OH
LOB	Line of Business
LOC	Localizer
LOM	Compass Locator at Outer Marker
Lr	Return Loss
LRU	Line Replaceable Unit
LUK	CINCINNATI, OH, AIRPORT, LUNKEN FIELD AIRPORT, ILS/DME
LWM	North Andover, MA, Combined Communications Center FIRE equipment
LXB	GREATER PITTSBURGH, PA, INTERNATIONAL ILS
M	Modem
M1FC	Model 1 Full Capacity
MA	Flight assistance dial access circuit
MACS	Message Authentication Codes
MALS	Medium-Intensity ALS
MALSR	Medium-Intensity ALS with Runway Alignment Indicator Lights (RAIL)
MBL	MANISTEE, MI, VOR/DME, MANISTEE COUNTY-BLACKER AIRPORT
Mbps	Megabits per second
MBS	SAGINAW, MI, TRICITY INTERNATIONAL AIRPORT, ILS
MC	Master Clock
MCC	Maintenance Control Center
MCH	BELLEVILLE, MI, GNAS
MCU	GREATER ROCHESTER, NY, INTERNATIONAL ILS or Multipoint Control Unit
MCU	Multi-point Control Unit
MD5	Message Digest 5
MDS	Master Demarcation System
MDT	Maintenance Data Terminal
METI	Meteorological Information: Weather-related information.
MF	AUTOVON circuits
MF	More Fragments
MFD	LAHM MUNICIPAL AIRPORT, BASE OPS, ILS, VORTAC, MANSFIELD, OH
MFDA	MANSFIELD, OH, RCO or MT. HOPE, OH, RCAG
MFDB	MANSFIELD, OH, RCAG
MG	Dedicated weather network circuits (WCP, RWP, WMSCR, WMP)
MGCP	Media Gateway Control Protocol
MGW	MORGANTOWN, WV, FSS, ILS, VORTAC; WALTER L BILL HART FIELD
MH	Dial-up ASOS circuits
MI	Public dial access to ATIS
MI	Michigan
MIDO	Manufacturing Inspection District Office
MIME	Multipurpose Internet Mail Extension
MISC	Miscellaneous: Used as a temporary service description until an appropriate service can be assigned.

TERM	Definition
MK20	Mark-20, upgraded ILS capability
MKG	MUSKEGON, MI, VORTAC, WSO; MUSKEGON COUNTY AIRPORT, ILS
MKGB	MUSKEGON, MI, RCO
MLTDP	Multidrop circuit
MM	Middle Marker or PDC for miscellaneous dial access lines for voice
MMDS	Multichannel Multipoint Distribution Service
MMS	Maintenance Management System
MMUSIC	Multi-party Multimedia Session Control
MNN	MARION, OH, MUNICIPAL AIRPORT
MNS	Mission Need Statement
MNTC	Maintenance Monitoring Service: Assets used for maintenance, network re-configuration, and/or monitoring facilities and services.
MODE-S	Mode Select Beacon System
MOP	MOUNT PLEASANT, MI, MUNICIPAL AIRPORT, VOR/DME
MOS	Mean Opinion Score
MP-MLQ	Multi-Pulse Maximum Likelihood Quantization
MPLS	Multi Protocol Label Switching
MPP	Multiple Point to Point network access
MPS	Maintenance Processor Subsystem
MRA	Mutual Recognized Arrangements
MRC	Monthly Recurring Cost
ms	millisecond(s)
ms	microsecond(s)
MS-CHAP	Microsoft Challenge Handshake Authentication Protocol
msec	microsecond(s)
MSN	MADISON, WI, VORTAC; DANE COUNTY REGIONAL-TRUAX FIELD AIRPORT, ILS
MTBF	Mean Time Between Failure
MTC	SELFRIEDGE ANGB AIRPORT, BASE OPS, ILS, TACAN, MT CLEMENS, MI
MTTF	Mean Time To Failure
MTU	Maximum Transmission Unit
MUX	Multiplexer
MW	INWATS (800) flight assistance service
MWO	HOOK FIELD MUNICIPAL AIRPORT, LOCALIZER, MIDDLETOWN, OH
N/A	Not Applicable
N97	CLEARFIELD-LAWRENCE AIRPORT, CLEARFIELD, PA
NACKS	Negative acknowledgements
NADIN	National Airspace Data Interchange Network
NADSW	NADIN Switch
NAMS	NADIN Message Processing Service (NADIN MSN)
NAS	National Airspace System
NAS	Naval Air Station
NASWIN	NAS-Wide Information Network
NAT	Network Address Translation
NAVAID	Navigational Aid
NAVMN	Navigation Monitor and Control
NB	AUTODIN circuits
NDB	Non-Directional Radio Homing Beacon
NDNB	National Airspace Data Interchange Network (NADIN II - PSN)
NEXCOM	Next Generation Air/Ground Communications
NEXRAD	Next Generation Weather Radar

TERM	Definition
NG	Multiplexing - exchange service dial backup circuits
NIC	Network Interface Card
NIMS	NAS Infrastructure Management System
NL	Dial-up LABS circuits
NM	Miscellaneous dial - access lines for data
NMCE	Network Monitor and Control
nmi	Nautical mile(s)
NN	NADIN 1A dial backup circuits
NOAA	National Oceanic and Atmospheric Administration
NOCC	Network Operational Control Center
NORAD	North American Aerospace Defense Command
NOTAM	Notice to Airmen
NPA/NXX	Area Code/Exchange acronym
NRC	Non Recurring Cost
NRCS	National Radio Communications System
NSM	Network Management System
NSTB	National Satellite Test Bed
NTIA	National Telecommunications and Information Agency
NTP	Network Time Protocol
NWS	National Weather Service
NXRAD	NWS Next Generation Radar
NXRD	Next Generation Weather Radar
OC	Optical Carrier
OCC	Operational Control Center
ODAPS	Oceanic Display and Processing System
OEX	OKLAHOMA CITY, OK, AERONAUTICAL CENTER
OH	Ohio
OHI	FAIRVIEW PARK, OH, GNAS
OK	Oklahoma
OM	Outer Marker
OMB	Office of Management and Budget
OPS	Operational or Operations
OPSW	Operational Switch
ORA	Organizational Registration Authorities
OSI	WOODSIDE, CA, VORTAC
OSI	Open Systems Interconnect
OSPF	Open Shortest Path First
OSTS	Operational Support Telephone System
OTS	Operational Telephone System
OVR	Override
OYM	ST MARYS, PA, MUNICIPAL AIRPORT
P/F	Phase/Frequency
P53	ROSTRAVER AIRPORT, MONONGAHELA, PA
PA	Pennsylvania
PABX	Private Automatic Branch Exchange
PAMRI	Peripheral Adapter Module Replacement Item
PAP	Password Authentication Protocol
PAPI	Precision Approach Path Indicator
PAT	IP Port Translation
PATH	A message type in the IP based protocol, RSVP, which transmitting applications send towards receivers. These messages describe the data that will be transmitted and the path that the data will take.

TERM	Definition
PBRF	Pilot Briefing
PBX	Private Branch Exchange
PC	Personal Computer
PCM	Pulse Code Modulation
PCR	Peak Cell Rate
PDC	Program Descriptor (or Designator) Codes
PDD	Presidential Directive
PEO	PENN YAN, NY, AIRPORT
PHB	Per Hop Behavior
PHD	HARRY CLEVER FIELD AIRPORT, NEW PHILADELPHIA; OH
PHN	PORT HURON, MI, AIRPORT
PIDP	Programmable Indicator Data Processor
PIT	PITTSBURGH, PA, INTERNATIONAL AIRPORT
PKI	Public Key Infrastructure
PLN	PELLSTON, MI, REGIONAL AIRPORT OF EMMET COUNTY AIRPORT, ILS; PELLSTON VORTAC
PLNA	HARBOR SPRINGS, MI, NRCS
PM	Post Meridiem , Latin words for after noon
PMM	PULLMAN, MI, VOR/DME
PON	Passive Optical Network
POP	Point of Presence
PoP	Point of Presence
POTS	Plain Old Telephone Service, the regular telephone service.
PPP	Point to Point Protocol
pps	Pulses per second
PPTP	Point-to-Point Tunneling Protocol
PQ	Priority Queuing
PRC	Peak Cell Rate
Prec	Precision
PRI	Primary Rate Interface, one of two types of ISDN services
PROGRAM_DE	Program Designator Code
PRS	Primary Reference Source
PSI	PONTIAC, MI, VORTAC
PSN	Packet Switched Network
PSN	Packet Switch Node
PSTN	Public Switched Telephone Network
PTK	OAKLAND COUNTY AIRPORT, PONTIAC, MI
PTKA	PONTIAC, MI, ATCT
PTN	Public Telephone Network
PTT	Push-To-Talk
PUP	Principal User Position
PVC	Permanent Virtual Circuit
PVM	Remote Terminal Access to Host Computer at FAATC (on DMN diagrams)
PWK	Wheeling Call Center (Fire Department), Wheeling, IL
QCF	CLEARFIELD, PA, ARSR
QD4	FAA RTR site in Pemberville, OH
QDT	CANTON, MI, ARSR
QoS	Quality of Service
QPL	THE PLAINS, VA, ARSR
QTA	ALGONAC, MI, RCAG
QTZ	LAGRANGE, IN, ARSR
QWO	CATAWBA, OH, ARSR

TERM	Definition
QWO	LONDON, OH, ARSR
QXU	REMSSEN, NY, ARSR
R	Receive loss
RADAR	NWS Radar, excluding NXRAD.
RADIUS	Remote Authentication Dial-In User Service
RAIL	Runway Alignment Indicator Lights
RAPCO	Radar Approach Control
RAS	Remote Access Server
RAS	Remote Access Server
RBDPE	Radar Beacon Data Processor Equipment
RC4	RSA Rivest Cipher 4 Algorithm
RC5	RSA Rivest Cipher 5 Algorithm
RCAG	Remote Communications Air/Ground Facility
RCE	Radio Control Equipment
RCIU	Remote Control Interface Unit
RCL	Radio Communications Link
RCLR	RCL Repeater
RCLT	RCL Terminal
RCO	Remote Communications Outlet
RDAT	Digitized Radar Data
RDP	Radar Display Processor
RED	Random Early Detection
REIL	Runway End Identification Lights
RESID	Private residence
RESV	Reservation Request, an RSVP message
RF	Radio Frequency
RFC	Request for Comments
RIP	Routing Information Protocol
RIPE	Reseaux IP Europeens
RISC	Reduced Instruction Set Computer
RIU	Radio Interface Unit
RKA	ROCKDALE, NY, VOR/DME
RLR	Receiver Loudness Rating
RMA	Reliability, Maintainability, and Availability
RME	GRIFFISS AIRFIELD AIRPORT, BASEOPS, ILS, ROME, NY
RML	Radar Microwave Link
RMLT	Radar Microwave Link Terminal
RMM	Remote Maintenance Monitoring
RMMS	Remote Maintenance Monitoring System
RMON	Remote Monitoring
RMS	Remote Monitoring Subsystem
RMVC	Remote Maintenance VORTAC Concentrator
RO	Regional Office
ROC	GREATER ROCHESTER, NY, INTERNATIONAL AIRPORT, ILS, VORTAC
ROD	ROSEWOOD, OH, VORTAC
RS	Recommended Standard
RSA	RSA algorithm was invented in 1978 by Ron Rivest, Adi Shamir, and Leonard Adleman
RSCS	File Transfer (on DMN diagrams)
RSVP	Resource Reservation Protocol
RTAD	Remote Tower Alphanumeric Display

TERM	Definition
RTCP	Real-time Control Protocol
RTP	Real-time Transport Protocol
RTR	Remote Transmitter/Receiver
RTRD	Remote Tower Radar Display
RVR	Runway Visual Range
RWDS	Remote Radar Weather Display Service
Rx	Receive
S/MIME	Secure Mutipurpose Internet Mail Extension
SAMS	Special Use Airspace Management
SAT	Satellite
SBM	Subnet Bandwidth Management
SBN	MICHIANA REGIONAL TRANSPORTATION CENTER AIRPORT, ILS, WSO
SCC	System Command Center
SCR	Sustainable Cell Rate
SD	Situational Display
SDP	Service Delivery Point
SERVICE_TY	Service Type code
SET	Secure Electronic Transaction
SF	Single-frequency (SF) signaling: In telephony, signaling in which dial pulses or supervisory signals are conveyed by a single voice-frequency tone in each direction
SGCP	Simple Gateway Control Protocol
SGH	SPRINGFIELD, OH, VOR/DME; SPRINGFIELD-BECKLEY MUNICIPAL AIRPORT, LOC/GS
SHA	Secure Hashing Algorithm
SIP	Session Initiation Protocol
SKY	SANDUSKY, OH, VOR/DME; GRIFFING SANDUSKY AIRPORT
SKY-1	Designator for the node comprising FAA facilities at the Sandusky RCAG Site
SKY-2	Designator for the node comprising FAA facilities at the Sandusky RCO/VDME Site
SLA	Service Level Agreement
SLC	SALT LAKE CITY, UT, NADIN CENTER, VORTAC; SALT LAKE CITY INTERNATIONAL AIRPORT, ILS/DME
SLD	Second-Level Domains
SLR	Speaker Loudness Rating
SMO	Systems Management Office
SNA	Systems Network Architecture
SNMP	Simple Network Management Protocol
SNMP	Simple Network Management Protocol
SOC	Service Operations Center
SOCKS	SOCK-et-S (An internal NEC development name that remained after release)
SONET	Synchronous Optical Network
SQL	Structured Query Language
SSALR	Simplified Short Approach Lighting System
SSC	System Support Center
SSL	Secure Socket Layer
SSU	System Support Unit
STARS	Standard TRACON Automation Replacement System
STM	Synchronous Transport Module
Strat	Stratum
STVS	Small Tower Voice Switch

TERM	Definition
SVC	Service Code
SVC	Switched Virtual Circuit
SVFA	Service F Interphone: Center to Center: Interphone service between ARTCCs.
SVFB	Service F Interphone: Center to Terminal: Interphone service between ARTCC and non-ARTCC facility.
SVFC	Service F Interphone: Non-ARTCC to Non-ARTCC: Interphone service between two non-center facilities.
SVFD	Service F Interphone: Miscellaneous interphone services
SVM	SALEM, MI, VORTAC
SYR	SYRACUSE, NY, VORTAC; SYRACUSE HANCOCK INTERNATIONAL AIRPORT
T	Transmit loss
T1	Trunk level 1, the North American designator for digital signal level 1, operating at a signaling rate of 1,544 Mbps and capable of handling 24 voice channels.
TACAN	Tactical Air Navigation Equipment
TBD	TIBBY VORTAC, THIBODAUX, LA
TCE	Tone Control Equipment
TCOM	Terminal Communications
TCP	Transport Control Protocol
TDLS	Tower Data Link Services (on DMN Diagrams)
TDMA	Time Division Multiple Access
TDMUX	Time Division Data Multiplexer
TDWR	Terminal Doppler Weather Radar
TDZ	METCALF FIELD AIRPORT, TOLEDO, OH
TELCO	Telephone Company
TELECOM_OF	Telephone Officer code in TIMS database
TELR	Talker Echo Loudness
TFAC	To FACility
TI	Tunnel Initiator
TIMS	Telecommunications Information Management System
TL5	TL Security (a small security company) Algorithm
TLD	Top-Level Domain
TLID	To Location IDentifier
TMA	HENRY TIFT MYERS AIRPORT, ILS/DME, TIFTON, GA
TMAS	Traffic Management Advisory System
TMCC	Traffic Management Computer Complex
TML	Television Microwave Link
TMLR	Television Microwave Link Repeater
TMLT	Television Microwave Link Terminal
TNAV	Terminal Navigational Aids
TOL	TOLEDO, OH, EXPRESS AIRPORT, BASE OPS, ILS, TOLEDO TACAN
TOS	Type of Service
ToS	Type of Service
TOTAL_MRC	Total Monthly Recurring Cost
TPX-42	A military numeric beacon decoder system
TRAC	TRACON
TRACO	Terminal Radar Approach Control
TRACON	Terminal Radar Approach Control Facility
TRAD	Terminal Radar Service
TRNG	Training: Consists of all information associated with training.
TSU	Traffic Simulation Unit

TERM	Definition
TSYS	Terminal Equipment Systems: Involves switches located at terminal facilities.
TT	Tunnel Terminator
TVC	TRAVERSE CITY, MI, VORTAC; CHERRY CAPITAL AIRPORT, ILS
TVCB	TIMS LID for TVC RCO
TWIP	Terminal Weather Information for Pilots
TWR	Tower. Non-FAA ATCT
Tx	Transmit
UAC	User Agent Client
UAS	User Agent Server
UB	Alarm and monitor circuits for other than ATC systems
UBR	Unspecified bit rate
UC	NADIN II data circuits
UCA	ONEIDA COUNTY AIRPORT, ILS, UTICA, NY, FSS, VORTAC
UCAC	UTICA, NY, RCO
UDP	User Datagram Protocol
UF	Critical DMN circuits (e.g., RDAT, BDAT, IDAT, FDAT, RMMS, etc.)
UG	Non-critical maintenance management circuits
UH	Critical monitor and control circuits (For example, ARSR, ILS, VOR)
UHF	Ultra High Frequency
UL	Non-critical DMN circuits for ASOS, CBI, MMS and FSAS
ULW	ELMIRA, NY, VOR/DME
UM	Miscellaneous circuits
UN	National Satellite Test Bed data circuits for satellite navigation
UNI	User Network Interface
UNIA	OHIO UNIVERSITY AIRPORT, LOC, ATHENS/ALBANY, OH
UNIX	UNIX [™] : A portable, multiuser, time-shared operating system that supports process scheduling, job control, and a programmable user interface. Note 1: There are many proprietary operating systems that are based on UNIX [™] and are colloquially referred to as UNIX [™] , but are not necessarily interoperable
UP	Non-critical T1 access circuits
URET	User Request Evaluation Tool
US	Critical T1 access circuits or United States of America
USDA	US Department of Agriculture site connected with the FAA
USNO	U.S. Naval Observatory
UTC	Coordinated Universal Time
UX	Wide Area Augmentation System (WAAS) circuits
UY	LINCS support assets
UZ	Equipment and services for Environmental Remote Monitoring System (ERMS)
VBR	Variable-bit rate
VCET	VSCS Console Equipment Trainer
VIDEO	FTS 2000 ISDN Video Conferencing Network service code
VDF	VSCS Distribution Frame
VDL	VHF Digital Link
VDME	VOR With Distance Measuring Equipment
VF	Data Multiplexing equipment
VFO	Voltage Control Oscillator
VFR	Visual Flight Rules
VFSS	Voice Frequency Signaling System
VG	DMN equipment Phase III
VG-8	Voice Grade circuit, 19.2 kbps bandwidth
VHF	Very High Frequency
VIC	Voice Interface Card

TERM	Definition
VK	FAA Telecommunications Satellite (FAATSAT) equipment
VLAN	Virtual LAN
VN	Version Number
VNAV	Visual Navigational Aids
VNM	Voice Network Module
VNTSC	Volpe National Transportation Systems Center
VoIP	Voice over IP, the transmission of voice signals over a packet data network
VOR	VHF Omnidirectional Range equipment
VORTAC	VOR Collocated with TACAN
VOT	VOR Test Facility
VPLAN	Virtual Private LAN
VPN	Virtual Private Network
VS	Voice Switch
VSCS	Voice Switching and Control System
VTAC	TACAN Collocated with VOR
VTs	Voice Telecommunication System
VWV	WATERVILLE, OH, VOR/DME
VX	High Capacity multiplexing, cross connect, and support equipment
WA	Next Generation Weather Radar (NEXRAD) circuits
WAAS	Wide Area Augmentation System
WAN	Wide Area Network
WARP	Weather Analysis Radar Processor
WC	Terminal Doppler Weather Radar (TDWR) circuits
WFQ	Weighted Fair Queuing
WJHTC	William J. Hughes Technical Center
WME	Wind Measuring Equipment
WMS	Master Stations
WMSCR	Weather Message Switching Center Replacement
WRED	Weighted Random Early Detection
WRS	Wide-area Reference Stations
WS	Work Station
WSCMO	Weather Service Contract Meteorological Observatory
WSFO	Weather Service Forecast Office
WSO	Weather Service Office
WWW	World Wide Web
XFSS	Auxiliary Flight Service Station
XUB	YELLOW BUD VORTAC, CIRCLEVILLE, OH
XX	Transmission that can not otherwise be categorized
YHM	HAMILTON, ONT, AIRPORT
YIP	WILLOW RUN AIRPORT, ILS/DME, DETROIT, MI
YIPA	YPSILANTI, MI, ATCT
YNG	YOUNGSTOWN-WARREN, OH, REGIONAL AIRPORT
YQG	WINDSOR, ONT, AIRPORT, VOR/DME
YSN	ST. CATHERINE'S, ONT, AIRPORT
ZAB	ALBUQUERQUE, NM, ARTCC
ZAU	CHICAGO, IL, ARTCC
ZBW	BOSTON, MA, ARTCC
ZDC	WASHINGTON, DC, ARTCC
ZDV	DENVER, CO, ARTCC
ZFW	FORT WORTH, TX, ARTCC
ZID	INDIANAPOLIS, IN, ARTCC
ZJX	JACKSONVILLE, FL, ARTCC

TERM	Definition
ZLA	LOS ANGELES, CA, ARTCC
ZMA	MIAMI, FL, ARTCC
ZME	MEMPHIS, TN, ARTCC
ZMP	MINNEAPOLIS, MN, ARTCC
ZNY	NEW YORK, NY, ARTCC
ZOB	CLEVELAND, OH, ARTCC
ZYZ	LESTER B. PEARSON INTERNATIONAL ACC, TORONTO, ONT. TORONTO CENTER ARTCC
ZZV	ZANESVILLE, OH, MUNICIPAL AIRPORT

ENDNOTES

¹ *Federal Aviation Administration Telecommunications Infrastructure, Mission Need Statement Number 322*, January 30, 1998, pp. 3-4.

² Federal Aviation Administration (FAA) Telecommunications Infrastructure (FTI) Technical Guidance Document, August 23, 1999, p. 1.

³ *IP Network Design*, IBM International Technical Support Organization, Redbook SG24-2580-01, June 1999, p. 187.

⁴ *Ibid.* p. 188.

⁵ *INTERNET SECURITY POLICY: A TECHNICAL GUIDE*, (Draft), NIST Special Publication 800-XX, p. 65.

⁶ This section on firewall types was extracted from *INTERNET SECURITY POLICY: A TECHNICAL GUIDE*, (Draft), NIST Special Publication 800-XX, pp. 66-70. Because of its excellent treatment of the subject and because it relates NIST policy on firewalls, it has been used here with little editing.

⁷ *Unifying of Data and Telephony Networks With Internet Communications Architecture*, Nortel Networks White Paper, p. 4.

⁸ *IP Telephony Intergateway Protocols*, Alan Percy, *Communications Systems Design Magazine*, March 2000, Volume 6, No. 4.

⁹ Q4 1999 ATM Market Analysis, Report Number: CQ00-01M4, May 1999

¹⁰ *Shouldn't we be talking about voice over anything?*, Robert Dallas, *Communications News*, January 2000, p. 46.

¹¹ *IP Network Design*, IBM International Technical Support Organization, Redbook No. SG24-2580-01, June 1999, p. 119.

¹² IPv6 has two types of addresses: those that are called IPv4 compatible, and IPv6 only addresses. An IPv4-compatible IPv6 address is an IPv6 address, assigned to an IPv6/IPv4 node, which bears the high-order 96-bit prefix 0:0:0:0:0:0 (the notation here is that of RFC 1933, with each 0 representing a pair of octets), and an IPv4 address in the low-order 32-bits. IPv4-compatible addresses are used by the automatic tunneling mechanism. An IPv6-only address is the remainder of the IPv6 address space (i.e., an IPv6 address that bears a prefix other than 0:0:0:0:0:0).

¹³ "It's About Time," *GPS World*, February 2000, p. 32.

¹⁴ Derived from "NTP Architecture, Protocol and Algorithms" briefing by David L. Mills, University of Delaware

¹⁵ NAS Architecture Vision For the Communications Area, TR99048, January 2000.

¹⁶ IEEE Recommended Practice for Speech Quality Measurements, *IEEE Transactions on Audio and Electroacoustics*, pp. 227-246, Sept. 1969

¹⁷ Source: International Telecommunication Union Standardization Sector G.114, *Transmission Systems and media, General Recommendations on the transmission quality for an entire international telephone connection, One-way transmission time*, Figure B.3

¹⁸ NAS-SR-1000, pg. 3.6.1.A.5.a

¹⁹ A. Watson and M. A. Sasse, "Multimedia Conferencing via Multicast: Determining the Quality of Service Required by the End User," *Proc. Int'l. Workshop Audio-Visual Services. over Packet Networks*, Aberdeen, Scotland, Sept. 1997.

²⁰ *IEEE Communications Magazine*, April 2000, Vol. 38 No. 4, *Internet Telephony: Services, Technical Challenges, and Products*, Mahbub Hassan and Alfandika Nayandoro, pp. 96-104.

-
- ²¹ Recommendation G.113 – Transmission Impairments, International Telecommunication Union, Feb. 1996.
- ²² IEEE Communications Magazine, April 2000, Vol. 38 No. 4, Performance Evaluation of the Architecture for End-to-End Quality-of-Service Provisioning, Katsuyoshi Lida, p. 79
- ²³ IEEE Communications Magazine, April 2000, Vol. 38 No. 4, Performance Evaluation of the Architecture for End-to-End Quality-of-Service Provisioning, Katsuyoshi Lida, p. 78
- ²⁴ IEEE Communications Magazine, April 2000, Vol. 38 No. 4, Performance Evaluation of the Architecture for End-to-End Quality-of-Service Provisioning, Katsuyoshi Lida, p. 79
- ²⁵ Business Communications Review, Volume 29, Number 1, Voice-over-IP: Better and Better , January 1999, pp. 28-34
- ²⁶ Echo Cancellation for VoIP, John C. Gammel, Communications Systems Design, October 1999, pp. 44-49
- ²⁷ ITU-T Recommendation G.131 (08/96) - Control of talker echo
- ²⁸ Transporting Voice Over IP, The Issues of Quality, Echo and Latency, 1999 Mockingbird Networks White Paper
- ²⁹ PDD 63 specifically recommended that “the FAA act immediately to develop, establish, fund, and implement a comprehensive National Airspace System program to protect the modernized NAS from information-based and other disruptions, intrusions and attack.”
- ³⁰ *Information System Security Program*, U.S. Department of Transportation, FAA, AIO-400, Order 1370.82.
- ³¹ *Information System Security Architecture*, Version 1.0, FAA ASD, March 30, 2000.
- ³² *Wide Area Network Security*, (Draft) Department of Transportation, FAA, AOP-500, Order 1830.9, September 30, 1999.
- ³³ *Information System Security Architecture*, pp. 3-3 through 3-4.
- ³⁴ Ibid., pp. 6-17 through 6-18.
- ³⁵ Ibid., pp. 6-18 through 6-20.
- ³⁶ Ibid., pp. 6-28 through 6-38.
- ³⁷ Private IP assignments are taken from the document “Address Allocation for Private Internets”, RFC 1597, dated March 1994.
- ³⁸ Please note that any physical changes to network topologies may require private IP address changes.
- ³⁹ Proxy gateways at AWA, AMC, and AWP provide private IP address users with the ability to access the Internet.
- ⁴⁰ These addresses are assigned EXCLUSIVELY for NAS/ATC use. See the latest revision of ENET supplement ENET1370-020.1, “FAA Enterprise Network Internet Protocol Version 4 (IPv4) NAS Intranet Address Assignments”, dated March 30, 1998.
- ⁴¹ IP address ranges 172.x.0.x and 172.x.255.x are reserved by the ENOCC.
- ⁴² ENET1370-020.1, FAA Enterprise Network Internet Protocol Version 4 (IPv4) NAS Intranet Address Assignments, March 30, 1998
- ⁴³ The FAA’s Enterprise Network Program (ENET) is an agency-wide effort aimed at facilitating the emergence of a true Enterprise data telecommunications network for the FAA. ENET, managed by AIT-300, is a partnership between the Office of Information Technology (AIT), the Office of Systems Architecture and Program Evaluation (ASD), and the NAS Operations Program (AOP), the three organizations with primary responsibility for data telecommunications in the agency. In addition, ENET includes representatives from Regional and Field Offices, Technical and Aeronautical Centers as well as

Program Offices. Through a coordinated team effort, the ENET Program endeavors to plan, standardize and manage the acquisition, implementation and operation of the FAA Enterprise Network. The ENET Program also provides a technical forum for addressing difficult networking issues without bias towards location or individual programs. Significant progress has already been achieved in the form of network addressing and naming standards for the entire agency. FTI is addressing the issues of Enterprise Network Management and coordinating with ENET.

⁴⁴ ENET1370-005.1B, *FAA Enterprise Network Agency Internet Access Plan*, October 24, 1999

⁴⁵ A backbone is a primary shared communications path offered by commercial companies to serve multiple users and offering high-speed, highly reliable network services.

⁴⁶ NAS Architecture, Version 4, Federal Aviation Administration, Date - TBD

⁴⁷ NAS Communications Architecture of the Future Final Technical Report, June 1997, Federal Systems Integration and Management Center Federal Systems Integration Center (FEDSIM), Subtask 036 of contract 90070TND-02.

⁴⁸ NAS Communications Architecture – Design Alternatives, Stanford Telecommunications, Inc, TR98083, November 1998.

⁴⁹ NAS Architecture Vision for the Communications Area, ITT Industries, TR99048, January 2000.

⁵⁰ Federal Aviation Administration (FAA) Telecommunications Infrastructure (FTI) Technical Guidance Document, August 23, 1999.

⁵¹ Federal Aviation Administration (FAA) Telecommunications Infrastructure (FTI) Statement of Work, October 20, 1999.

⁵² Security requirements are addressed separately in Section 4 of this report.

⁵³ Trends Driving the New Access Network, Pair Gain Technology, www.pairgain.com/technology/nan_trends.asp.

⁵⁴ AT&T Encore News, First and Second Quarters 2000, www.att.com/retirees/encore/12q00/news05.html

⁵⁵ These facilities were selected from the TIMS database, as of May 15, 2000.

⁵⁶ *An Explanation of RMA Categories*, Reliability, Maintainability, and Availability in the FAA Telecommunications Infrastructure (FTI), May 10, 1999, FTI Engineering Team

⁵⁷ “IP Network Design Guide”, Murhammer, Lee, Motallebi, Borghi, and Wozabal, IBM International Technical Support Organization, June 1999.

⁵⁸ NAS Communications Architecture – Design Alternatives, TR98093, Stanford Telecommunications, Inc, November 1998 and NAS Architecture Vision for the Communications Area, TR99048, ITT Industries, January 2000.

⁵⁹ As described in Section 5.5.1, the proposed network architectures include a few nodes that retain direct connections to the PSTN. In these cases, the number and cost of PSTN connections was low, and the cost to install packet voice gateways and network interface equipment was not justified.

⁶⁰ NAS Architecture Vision for the Communications Area, ITT Industries, TR99048, January 2000.

⁶¹ NAS Architecture Vision for the Communications Area, ITT Industries, TR99048, January 2000, p. 3-104, Figure 3-48.

⁶² Reference Voice Switch Study, Dunbar, Rick

⁶³ Attachment J.6 (b), FTI Implementation and Transition Guidelines, DTFA01-00-S-00FTI, July 28, 2000, p. J.6 (b)-4.

⁶⁴ 179614A, Book IV of IV, Switching Subsystem Hardware Detailed Design Document (HWCI-2) for the Voice Switching and Control System (VSCS), 1 July 1992

⁶⁵ 179617A, Hardware Top Level Design Document for the Voice Switching and Control System (VSCS), 22 July 1992

-
- ⁶⁶ Trunk Anomalies Presentation, William A. Baker, ANM-450E2/NISC, 13 July 1994
- ⁶⁷ NAS-IC-42018404, VSCS to the Trunks Interface Control Document for the Voice Switching and Control System (VSCS), 10 October 1997, p. 6.
- ⁶⁸ Voice Switching and Control System, Attachment J-3, Product Specification, 12 November 1997, p. 68.
- ⁶⁹ Voice Switching and Control System, Attachment J-3, Product Specification, 12 November, 1997
- ⁷⁰ NAS Architecture Vision For The Communications Area, TR99048, January 2000, p. 3-97.
- ⁷¹ NAS Architecture Vision For The Communications Area, TR99048, January 2000, p. 3-98.
- ⁷² NAS Architecture Vision For The Communications Area, TR99048, January 2000, p. 3-90.
- ⁷³ Voice Switching and Control System, Attachment J-3, Product Specification, 12 November, 1997, p. 29
- ⁷⁴ Cisco 3600 Modular Router Configuration Guide, Configuring Voice Ports **VC-95**
- ⁷⁵ Attachment J.6 (b), FTI Implementation and Transition Guidelines, DTFA01-00-S-00FTI, July 28, 2000, p. J.6 (b)-3.
- ⁷⁶ The latency block diagram and associated calculations for Scenario 1B would be similar to those developed for Scenarios 1A and 2, with an extra connector (hop) added to the wide area network for FAA sites which connect to hub nodes prior to connection to the network backbone. This added connection accounts for ≤ 5 msec in latency.
- ⁷⁷ "A Modern Taxonomy of High Availability", Ron I. Resnick, 1996 as posted at www.interlog.com/~resnick/HA.htm
- ⁷⁸ Information obtain in Network Computing Magazine, February 7, 2000
- ⁷⁹ Cost Details for a Remote Site, Grant's Pass Pricing Agreement, www.telecom.das.state.or.us/data/pie001.htm
- ⁸⁰ Draft Future Telecommunications Infrastructure (FTI) Supplies or Services and Prices/Costs, System Requirements Document Part I – Section B, DTFA01-00-S-00FTI, 7/28/2000.
- ⁸¹ Ibid.
- ⁸² Upon conversations with equipment manufacturer Cisco, it was determined that a typical government discount is on the order of 55%.